Design Guide for Cisco Unity

Release 5.x
Revised May 6, 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-14619-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0501R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Design Guide for Cisco Unity Release 5.x
© 2008 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface ix

Audience ix

Document Conventions ix

Additional Cisco Unity Documentation, System Requirements, and Supported Hardware and Software x

Support Policy for Optional Third-Party Software x

Obtaining Documentation, Obtaining Support, and Security Guidelines xi

Cisco Product Security Overview xi

CHAPTER 1 **Design Guide Overview** 1-1

CHAPTER 2 **Cisco Unity Concepts** 2-1

How Cisco Unity Works 2-1

Characteristics of Unified Messaging and Voice Messaging Systems 2-2

Unified Messaging 2-2

Voice Messaging 2-2

Hardware Components of a Cisco Unity System 2-3

Cisco Unified Communications Manager or Another Supported Phone System 2-3

One or More Cisco Unity Servers 2-4

Voice Cards or PIMG Units (Required for Integrations with Circuit-Switched Phone Systems) 2-4

Expansion Chassis (Required Only for Some Integrations with Circuit-Switched Phone Systems) 2-4

One or More Message-Store Servers (Optional for Some Configurations) 2-5

One or More Dedicated Domain Controllers/Global Catalog Servers (Exchange Only, Large Voice Messaging Configurations Only) 2-5

Cisco Unity Bridge Server (Required Only for Interoperating with Avaya Voice Messaging Systems) 2-5

Network Connection (Optional for Some Configurations) 2-5

Software Components of a Cisco Unity System 2-6

Where Cisco Unity Stores Data 2-6

Voice Messages Are Stored in Domino or Exchange 2-6

All Subscriber Information Is Stored in a SQL Server 2000 Database 2-7

Some Subscriber Information Also Appears in the Domino Address Book or in Active Directory 2-8

Data That Appears in Both the SQL Server 2000 Database and in the Address Book/Directory Is Automatically Synchronized 2-9

Messages from Outside Callers Are Temporarily Stored on the Cisco Unity Server 2-10

Some Subscriber Information and Configuration Settings Are Stored on the Cisco Unity Server 2-10
Some Configuration Settings Are Stored in the Registry 2-10

CHAPTER 3 **Network Infrastructure Requirements 3-1**
Availability of Network Resources 3-1
Name Resolution 3-1
Domain Controller Access and Availability 3-2
Availability of Message Store Servers 3-2
Using Firewalls with Cisco Unity 3-3
Sizing and Scaling Cisco Unity Servers 3-3
Maximum Number of Users on Dedicated Domino or Exchange Servers 3-4
Storage Capacity for Voice Messages 3-4
Number of Voice Ports 3-4
Audio Codecs 3-5
How Codecs Affect the File Size of Voice Messages 3-5
TTS, TTY, Pocket PCs, and Hand-Held Computers 3-6
Interoperability Among Multiple Voice-Messaging Systems 3-6

CHAPTER 4 **Designing a Cisco Unity System with Exchange as the Message Store 4-1**
Deployment Models 4-1
Unified Messaging with Customer-Provided Infrastructure 4-2
Mixed Unified Messaging and Voice Messaging with Customer-Provided Infrastructure 4-2
Voice Messaging with Cisco-Provided, Dedicated Infrastructure 4-2
Voice Messaging with Customer-Provided Infrastructure 4-3
Multi-Site WAN with Distributed Messaging 4-3
Physical Placement and Network Infrastructure 4-4
Considerations for Customer-Provided Infrastructure 4-5
Active Directory Considerations 4-5
Exchange Considerations (All Versions) 4-7
Exchange Considerations That Apply Only Exchange 2007 4-8
Considerations for Cisco-Provided, Dedicated Infrastructure 4-9

CHAPTER 5 **Designing a Cisco Unity System with Domino as the Message Store 5-1**
Overview of Cisco Unity with Domino and Notes 5-1
Maximum Number of Cisco Unity Subscribers 5-2
Domino Address Book Terminology 5-2
IBM Lotus Domino Unified Communications (DUC) for Cisco on Domino Servers and on Client Workstations 5-2
Address Book Server, Message Store Server, and Mail Drop Server 5-4

Windows Domains and Domino Domains 5-5
Server Placement 5-5
Active Directory Accounts and Permissions 5-6
Authentication 5-6
Domino Permissions 5-7
Cisco Unity Subscribers and Domino Users 5-7
Domino Clusters 5-7
Message Routing 5-8
Notes Client on the Cisco Unity Server 5-8
Client Access Licenses 5-8
Backing Up and Restoring Data 5-8
Migrating from Cisco Unity for Exchange 5-8
Cisco Unity and the Domino Address Book 5-8
Unified Messaging Configurations 5-9
Unified Messaging, No Domino Cluster 5-9
Unified Messaging, Domino Cluster 5-10
Voice Messaging Configuration 5-10
Criteria for a Supported Configuration 5-10
Deploying Cisco Unity for Lotus Domino 5-11
Administrative Access and Control 5-12
Establishing Support Policies 5-12
Network Services 5-12
Deployment Tasks for Unified Messaging Configurations 5-12
Operational Tasks 5-13
Feature Parity Between Cisco Unity for Domino and Cisco Unity for Exchange 5-14

CHAPTER 6 **Integrating Cisco Unity with the Phone System** 6-1
Overview 6-1
How an Integration Works 6-2
Lines and Cables to Make Physical Connections 6-3
Settings in the Phone System and in Cisco Unity 6-7
Call Information Exchanged by the Phone System and Cisco Unity 6-7
Call Control 6-8
Sample Path for a Call from the Phone System to a Subscriber 6-8
General Integration Issues 6-9
Integrating with Cisco Unified Communications Manager (by Using SCCP or SIP) 6-10
Integrating Cisco Unity with Multiple Versions of Cisco Unified Communications Manager 6-11
Integrating Cisco Unity with Multiple Cisco Unified Communications Manager Clusters 6-12

Cisco Unified Communications Manager Authentication and Encryption for Cisco Unity Voice Messaging Ports (SCCP Integrations Only) 6-12
Packetization (SCCP Integrations Only) 6-17
Integrating with Cisco Unified Communications Manager Express (by Using SCCP or SIP) 6-17
Multiple Cisco Unified Communications Manager Express Version Support 6-18
Multiple Cisco Unified Communications Manager Express Routers Integrating with a Single Cisco Unity Server 6-19
Integrating Cisco Unity with Cisco Survivable Remote Site Telephony (Cisco SRST) 6-19
Integrating by Using SIP 6-22
Supported SIP Integrations 6-23
Cisco Unity Failover with SIP Trunks 6-23
SIP Compliance 6-23
Integrating with Circuit-Switched Phone Systems by Using PIMG or TIMG Units 6-24
Description of PIMG Integrations 6-24
Description of TIMG Integrations 6-26
Setup and Configuration 6-27
Firmware Updates 6-27
Serial Integrations 6-27
Increasing Port Capacity 6-28
Cisco Unity Failover 6-28
Cisco Unity Failback 6-29
Multiple Integration Support/Branch Office Consolidation 6-29
Integrating with Multiple Phone Systems 6-30
Requirements for Integrations with Multiple Phone Systems 6-31
Using SCCP Phone Systems with Other Integrations 6-31
Notes for PIMG Integrations 6-31
Optional Integration Features 6-32
Alternate Extensions 6-32
Alternate MWIs 6-33
Centralized Voice Messaging 6-34

CHAPTER 7 **Cisco Unity Failover and Standby Redundancy** 7-1
Comparison of Cisco Unity Failover and Standby Redundancy 7-1
Failover 7-1
Configuring Failover When Cisco Unity Servers Are Separated by a Firewall 7-2
Installing Exchange 2003 on the Cisco Unity Secondary Server in a Voice Messaging Configuration with Failover 7-2
Requirements for Spanning a Cisco Unity Failover Pair Across Redundant Data Centers 7-2
Standby Redundancy 7-2

Installing Exchange 2003 on the Cisco Unity Primary Server in a Standby Redundancy Configuration 7-3
Diagram of a Standby Redundancy Configuration 7-5

CHAPTER 8 **Voice-Recognition Access to Cisco Unity** 8-1

CHAPTER 9 **Migrating to Cisco Unity from Another Voice-Messaging System** 9-1

INDEX

Preface

See the following sections:

- Audience, page ix
- Document Conventions, page ix
- Additional Cisco Unity Documentation, System Requirements, and Supported Hardware and Software, page x
- Support Policy for Optional Third-Party Software, page x
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page xi

Audience

The *Design Guide for Cisco Unity Release 5.x* is intended for anyone responsible for the design or configuration of a Cisco Unity system.

Document Conventions

The *Design Guide for Cisco Unity Release 5.x* uses the following conventions:

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the document.

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Additional Cisco Unity Documentation, System Requirements, and Supported Hardware and Software

For descriptions and the URLs of Cisco Unity documentation on Cisco.com, see the *Documentation Guide for Cisco Unity*. The document is shipped with Cisco Unity and is available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_documentation_roadmaps_list.html.

In particular, note:

- For system requirements, and lists of supported hardware and software, the *System Requirements for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
- For a list of servers that meet Cisco Unity specifications, the *Cisco Unity Supported Platforms List*, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.
- For client workstations, a list of the software that is compatible with the version of Cisco Unity that you are installing, and a list of messaging clients that are compatible with the version of Cisco Unity that you are installing, the *Compatibility Matrix: Cisco Unity and the Software on Subscriber Workstations* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html.

Support Policy for Optional Third-Party Software

The Cisco support policy states that customers can deploy third-party software for backup, monitoring, and security on the Cisco Unity server. However, Cisco expects that customers (or their systems integration partners) will have tested the interoperability of such products with Cisco Unity before the products are deployed. Such testing is essential in mitigating the risk that problems between Cisco Unity and the third-party products loaded on the Cisco Unity server will be discovered within the production environment.

If a customer calls the Cisco Technical Assistance Center (TAC) with a problem, a Cisco TAC engineer may require that optional third-party software be turned off or even removed from the Cisco Unity server during the course of troubleshooting. If it is determined that the interoperability between the third-party software and Cisco Unity was the root cause of the problem, the Cisco TAC engineer will require that the third-party software be disabled or removed from the Cisco Unity server until the interoperability issue is addressed so that the customer can continue to have a functional Cisco Unity system.

Before installing any qualified optional Microsoft service pack on the Cisco Unity server, confirm that the manufacturer of any optional third-party software or hardware that you plan to install on the Cisco Unity server—or that is already installed—also supports the service pack for use with its product.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products can be found at http://www.cisco.com/wwl/export/crypto/tool/stqrg.html. If you require further assistance, contact us by sending e-mail to export@cisco.com.

CHAPTER 1

Design Guide Overview

The following table lists the feature areas that affect the design of a Cisco Unity system and, for each area, the location where you will find more information (either in this guide or in other Cisco Unity documentation). Note that for some features, documentation that covers only system design is not available; therefore, the location listed is for feature documentation.

Product Area	Design or Feature Documentation
Cisco Unity concepts	Chapter 2, "Cisco Unity Concepts"
Network infrastructure requirements	Chapter 3, "Network Infrastructure Requirements"
Cisco Unity with Microsoft Exchange as the message store	Chapter 4, "Designing a Cisco Unity System with Exchange as the Message Store"
Cisco Unity with IBM Lotus Domino as the message store	Chapter 5, "Designing a Cisco Unity System with Domino as the Message Store"
Integrating Cisco Unity with the phone system	• Chapter 6, "Integrating Cisco Unity with the Phone System" • If Cisco Unity will be integrated with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager), see the applicable Cisco Unified CM SRND at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html.
Cisco Unity failover and standby redundancy	Chapter 7, "Cisco Unity Failover and Standby Redundancy"

Product Area	Design or Feature Documentation
Interoperating with or migrating from other voice-messaging systems	• For information on interoperating with Avaya voice-messaging systems, see the following documents: – The *Design Guide for Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_implementation_design_guides_list.html. – The applicable *Networking Guide for Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html. • For information on interoperating with other voice-messaging systems, see the applicable *Networking Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html. • For information on migrating from another voice-messaging system to Cisco Unity, see Chapter 9, "Migrating to Cisco Unity from Another Voice-Messaging System."
Security	For information on security for Cisco Unity, see the applicable version of the *Security Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.
Speech recognition	Chapter 8, "Voice-Recognition Access to Cisco Unity"
Client access to voice messages	• For end-user documentation on how Cisco Unity subscribers access Cisco Unity voice messages and change their own Cisco Unity settings, see the Cisco Unity End-User Guides section of the Cisco website at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html. • For information on setting up subscriber workstations, see the "Setting Up Subscriber Workstations" chapter in the applicable version of the *System Administration Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html. • For information on subscriber orientation, see the "Subscriber Orientation" chapter in the applicable version of the *System Administration Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html. • For information on authentication for Cisco Personal Communications Assistant (PCA), see the "Authentication for Cisco Unity Applications" chapter of the applicable *Security Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.
Using Groupwise	For information on using Novell GroupWise to access Cisco Unity voice messages, see the website for the third-party application GW-Unify, http://www.gwipt.com.
Sending and receiving faxes for Cisco Unity subscribers	For information on: • The IP Fax Configuration wizard, see http://ciscounitytools.com/App_IPFaxConfigurationWizard.htm. • Configuring Cisco Unity to work with external fax servers that support Exchange and/or Domino, see http://ciscounitytools.com/App_ThirdPartyFaxConfig.htm.

CHAPTER 2

Cisco Unity Concepts

- How Cisco Unity Works, page 2-1
- Characteristics of Unified Messaging and Voice Messaging Systems, page 2-2
- Hardware Components of a Cisco Unity System, page 2-3
- Software Components of a Cisco Unity System, page 2-6
- Where Cisco Unity Stores Data, page 2-6

How Cisco Unity Works

Cisco Unity is a unified messaging system that can also be a voice messaging system, and it requires a dedicated messaging infrastructure. When Cisco Unity subscribers are busy or away from their phones, Cisco Unity answers the phone and takes voice messages for them. The subscribers can retrieve their messages over the phone, or by using IBM Lotus Notes, Microsoft Outlook, the Cisco Unity Inbox, Cisco Unified Personal Communicator, or an IMAP client.

When a call comes in for a subscriber, the following occurs:

1. A caller dials the subscriber extension. If the subscriber phone is busy or the subscriber does not answer, the phone system routes the call and information about the call, including the subscriber extension, to Cisco Unity.
2. Cisco Unity answers the call, looks up the subscriber extension in the Cisco Unity database, retrieves and plays the subscriber greeting (“Hi, this is Pat, and I am not at my desk right now...”), and lets the caller leave a message.
3. When the caller ends the call, the message is temporarily saved on the hard disk on the Cisco Unity server.
4. Cisco Unity gives the message to Domino or Exchange, which routes the message to the subscriber home server and stores it in the subscriber mailbox. If the call is from:
   - Another subscriber, the message is identified as coming from that person.
   - An outside caller who has not logged on to Cisco Unity as a subscriber, the message is identified as coming from the Unity Messaging System mailbox.
5. Cisco Unity informs the subscriber in one or more of the following ways that a message has arrived, regardless of the source of the call. (This is unlike some voice messaging systems, which activate message waiting indicators only when a message is left over the phone.)
   - If the subscriber has a phone connected to the phone system, Cisco Unity activates the subscriber message waiting indicator (MWI).

Note This is true unless the MWI had already been activated because of a prior message arrival, in which case it simply remains activated.

- If the subscriber has configured personal notification options in the Cisco Unity Assistant, Cisco Unity can also call one or more phones or pagers, send an e-mail to a text pager, or send an SMS message to a mobile phone to notify the subscriber that a new voice message has arrived.

Characteristics of Unified Messaging and Voice Messaging Systems

Cisco Unity can be configured either for Cisco Unity Unified Messaging or for Cisco Unity Voice Messaging. This section enumerates the characteristics of each configuration.

Unified Messaging

- Cisco Unity voice messages are stored in the same IBM Lotus Domino or Microsoft Exchange message store in which e-mails and faxes (if applicable) are stored, so subscribers see all e-mails, voice messages, and faxes in the same Inbox.
- A supported version of IBM Lotus Domino or Microsoft Exchange must be installed on a separate server. (For information on supported versions, see *System Requirements for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
- The Cisco Unity server is connected to the network, so it has access to the message store, the directory (a Domino address book or Active Directory), and network utilities such as virus checking and backup.
- Subscribers check messages:
  - With Domino, by using the phone or an e-mail client.
  - With Exchange, by using the phone, the Cisco Unity Inbox, or an e-mail client. (The Cisco Unity Inbox is accessed through the Cisco Personal Communications Assistant, or Cisco PCA.)
- Cisco Unity administration can be performed over the network.
- Subscribers have access to the Cisco Unity Assistant through the Cisco PCA.
- Voice mail and e-mail attributes on subscriber accounts can be administered from a single location by using the Cisco Unity Administrator.
- Cisco Unity can play back electronic messages over the phone by using Text to Speech, and can support identifying, redirecting, and printing third-party faxes.

Voice Messaging

Revised May 6, 2008

- Voice messages are stored in a supported version of Microsoft Exchange or IBM Lotus Domino.

The message store contains only Cisco Unity voice messages, not e-mails or faxes.

Exchange can be installed either on the Cisco Unity server or on a separate server, depending on the number of subscribers that need to be supported by Cisco Unity. Domino must be installed on a separate server.

- Subscribers check messages:
  - With Domino or Exchange, by using the phone or Cisco Personal Communicator.
  - With Exchange, by using the Cisco Unity Inbox (accessed through the Cisco PCA) or an IMAP e-mail client.
- E-mail attributes, if any, and voice mail attributes on subscriber accounts must be administered separately.
- Cisco Unity can play back electronic messages over the phone by using Text to Speech, and can support identifying, redirecting, and printing third-party faxes.

Hardware Components of a Cisco Unity System

See the following sections:

- Cisco Unified Communications Manager or Another Supported Phone System, page 2-3
- One or More Cisco Unity Servers, page 2-4
- Voice Cards or PIMG Units (Required for Integrations with Circuit-Switched Phone Systems), page 2-4
- Expansion Chassis (Required Only for Some Integrations with Circuit-Switched Phone Systems), page 2-4
- One or More Message-Store Servers (Optional for Some Configurations), page 2-5
- One or More Dedicated Domain Controllers/Global Catalog Servers (Exchange Only, Large Voice Messaging Configurations Only), page 2-5
- Cisco Unity Bridge Server (Required Only for Interoperating with Avaya Voice Messaging Systems), page 2-5
- Network Connection (Optional for Some Configurations), page 2-5

Cisco Unified Communications Manager or Another Supported Phone System

Cisco Unity can be integrated with Cisco Unified Communications Manager (Cisco Unified CM) or another supported phone system. For a list of supported phone systems, see the applicable version of *Supported Hardware and Software, and Support Policies for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

For integrations with circuit-switched phone systems, the customer may require special cables, line splitters, and so on. For more information, see the integration guide for the phone system that the customer uses. Cisco Unity integration guides are available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Cisco Unity can also be integrated with multiple telephone systems. For more information, see the *Multiple Telephone System Integrations Guide for Cisco Unity 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

One or More Cisco Unity Servers

For a detailed list of servers that are qualified for use with Cisco Unity, see the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.

Each qualified Cisco Unity server can service a specified number of Cisco Unity subscribers depending on the type of server and, for Voice Messaging configurations, depending on whether Exchange is installed on the Cisco Unity server. The *Cisco Unity Supported Platforms List* indicates how many subscribers can be serviced by each type of server.

For Unified Messaging configurations, at least one Cisco Unity server is required for each:

- Domino domain
- Exchange organization

If the customer purchases Cisco Unity failover, two Cisco Unity servers are required:

- The primary server, which takes calls the majority of the time; and
- The secondary server, which takes calls when the customer wants to perform maintenance on the primary server or when the primary server stops functioning for any reason.

If the customer purchases Voice Recognition licenses, one voice-recognition server is required for each Cisco Unity server. For a list of servers that are qualified as voice-recognition servers, see the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.

Note Voice recognition is not supported with phone system integrations that use voice cards.

Voice Cards or PIMG Units (Required for Integrations with Circuit-Switched Phone Systems)

If the customer integrates Cisco Unity with a circuit-switched phone system, either voice cards or PIMG units are required. For a list of supported voice cards, see the *Supported Hardware and Software, and Support Policies for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Expansion Chassis (Required Only for Some Integrations with Circuit-Switched Phone Systems)

If the customer is integrating Cisco Unity with a circuit-switched phone system and needs more voice cards than will fit in the Cisco Unity server, an expansion chassis is required for the voice cards (see the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html for more

information). All voice cards must be installed in the expansion chassis; they cannot be split between the server and the expansion chassis, because all of the cards must be connected to one another by using a single H.100 cable.

One or More Message-Store Servers (Optional for Some Configurations)

For Cisco Unity systems configured for Unified Messaging, the message store software (IBM Lotus Domino or Microsoft Exchange) must be installed on a server other than the Cisco Unity server.

For Cisco Unity systems configured for Voice Messaging, Exchange can be installed on the Cisco Unity server or on a separate server. Domino must be installed on a separate server.

The number of subscribers homed on the Cisco Unity server cannot exceed the maximum listed for that type of server on the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.

One or More Dedicated Domain Controllers/Global Catalog Servers (Exchange Only, Large Voice Messaging Configurations Only)

For large Voice Messaging configurations, one or more dedicated domain controllers/global catalog (DC/GC) servers may be required. For more information, see Chapter 3, "Network Infrastructure Requirements."

Cisco Unity Bridge Server (Required Only for Interoperating with Avaya Voice Messaging Systems)

If the customer wants Cisco Unity to interoperate with an Avaya voice messaging system, a dedicated Cisco Unity Bridge server is required. For more information, see the following documents:

- For information on how Cisco Unity can send voice messages to Avaya and receive voice messages from Avaya, see the applicable version of the *Networking Guide for Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
- For requirements for connecting Cisco Unity and Avaya, see the *System Requirements, and Supported Hardware and Software for Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Network Connection (Optional for Some Configurations)

For Cisco Unity systems that are configured for Unified Messaging, a network connection is required.

For Cisco Unity systems that are configured for Voice Messaging, a network connection is required only if the customer wants to do one or more of the following:

- Use Domino for the message store.
- Integrate Cisco Unity with an IP phone system (for example, Cisco Unified Communications Manager).
- Administer Cisco Unity over the network.

- Give subscribers access to Cisco Unity by using the Cisco Unity Assistant, the Cisco Unity Inbox, an IMAP e-mail client, or Cisco Personal Communicator.
- Install Exchange on a separate server.

Note For a system with a large number of Cisco Unity subscribers, installing Exchange on a separate server is required.

- Give the Cisco Unity server access to network utilities such as virus checking and backup.

Software Components of a Cisco Unity System

For information on the software installed on the Cisco Unity server, the supported versions of Domino and Exchange, and the supported versions of client software, see the *System Requirements for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Where Cisco Unity Stores Data

Cisco Unity stores data in a variety of locations, as described in the following sections:

- Voice Messages Are Stored in Domino or Exchange, page 2-6
- All Subscriber Information Is Stored in a SQL Server 2000 Database, page 2-7
- Some Subscriber Information Also Appears in the Domino Address Book or in Active Directory, page 2-8
- Data That Appears in Both the SQL Server 2000 Database and in the Address Book/Directory Is Automatically Synchronized, page 2-9
- Messages from Outside Callers Are Temporarily Stored on the Cisco Unity Server, page 2-10
- Some Subscriber Information and Configuration Settings Are Stored on the Cisco Unity Server, page 2-10
- Some Configuration Settings Are Stored in the Registry, page 2-10

Voice Messages Are Stored in Domino or Exchange

Cisco Unity stores voice messages either in Domino mailfile databases or in Exchange message stores.

Domino

Cisco Unity stores voice messages in a user mail file database on the Domino server. Domino is installed on one or more servers (never on the Cisco Unity server); therefore, all subscribers have their Domino mailboxes on other servers. A Cisco Unity subscriber is someone who has a Domino mailbox and whose Domino person document includes Cisco Unity-specific information.

Every Domino server that homes Cisco Unity subscribers must have IBM Lotus Domino Unified Communications (DUC) for Cisco installed. At the time this document was written, DUC was available only for Windows 2000 Server, Windows Server 2003, and AIX. For information on operating systems

currently supported by DUC for Cisco, see the "Domino Requirements—Message Store" section of *System Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Cisco Unity can service subscribers on multiple Domino servers. You specify one Domino server (the partner Domino server) through which Cisco Unity communicates with the other Domino servers.

Cisco Unity can also service subscribers on Domino clusters. If subscribers are homed on one or more Domino servers in a cluster, every Domino server in the cluster on which there will be Cisco Unity subscribers must have DUC installed.

Exchange

Cisco Unity can store voice messages in supported versions of Exchange. For information on versions of Exchange currently supported for use with Cisco Unity, see the "Exchange Requirements—Message Store" section of *System Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

For small Cisco Unity Voice Messaging configurations, Exchange can be installed on the Cisco Unity server, and all Cisco Unity subscribers can have their Exchange mailboxes on the Cisco Unity server. (Exchange can also optionally be installed on a separate server instead of, or in addition to, being installed on the Cisco Unity server.) A Cisco Unity subscriber is someone who has an Exchange mailbox and whose Active Directory account includes Cisco Unity-specific information.

For medium and large Cisco Unity Voice Messaging configurations and for all Unified Messaging configurations, Exchange is installed on one or more separate servers instead of on the Cisco Unity server. For these configurations, subscribers can have their Exchange mailboxes on other Exchange servers.

Cisco Unity can service subscribers on multiple Exchange servers. You specify one Exchange server (the partner Exchange server) through which Cisco Unity communicates with the other Exchange servers. The partner Exchange server can either be the Cisco Unity server (when Exchange is installed on the Cisco Unity server) or a separate server.

For Exchange 2003, Cisco Unity can also service subscribers on both active/active and active/passive clusters. Do not install Cisco Unity on a server in an Exchange cluster.

All Subscriber Information Is Stored in a SQL Server 2000 Database

Cisco Unity stores all information about Cisco Unity subscribers, as well as selected Cisco Unity configuration data, in a SQL Server 2000 or Microsoft Data Engine 2000 (MSDE 2000) database on the Cisco Unity server. (The number of voice ports on the Cisco Unity server and, therefore, the maximum number of subscribers the server can support, determines whether data is stored in SQL Server 2000 or in MSDE, which is fully compatible with SQL Server 2000.)

When two or more Cisco Unity servers are in the same Domino domain and monitoring the same address book, or are in the same Active Directory forest, the SQL Server 2000 database on each Cisco Unity server also includes a small amount of information about all of the subscribers on the other Cisco Unity servers.

Storing subscriber data in a SQL Server 2000 database has the following benefits:

- **Performance:** Because the SQL Server 2000 database is on the Cisco Unity server itself and because the data is heavily indexed, accessing data—including looking up subscriber extensions—is fast. The current maximum number of Cisco Unity subscribers in a Domino address book or Active Directory Global Address List is 250,000.

- **Reliability:** Because subscriber data is stored on the Cisco Unity server, Cisco Unity can answer calls, let outside callers look up subscriber extensions, and take messages even when the Domino or Exchange network is down. (When the Domino or Exchange network is unavailable, new messages are stored on the Cisco Unity server, and subscribers have access to those messages.)
- **Scalability:** SQL Server 2000 was designed to support the largest enterprise data processing systems, so there is more than enough room for storing the Cisco Unity data. Although MSDE has storage limitations that SQL Server does not, it is also more than adequate for the Cisco Unity configurations for which it is sold.
- **Network Impact:** Only a small subset of subscriber information needs to be stored in the directory, and that information does not change frequently. Therefore, directory replication caused by changes to Cisco Unity data is minimal after subscriber accounts have been created.

Some Subscriber Information Also Appears in the Domino Address Book or in Active Directory

A small amount of data that appears in the SQL Server 2000 database also appears in the Domino address book or in Active Directory. This information, mostly subscriber data (including the recorded voice name), is added to the directory to enable Cisco Unity servers to communicate with one another and to enable communication between Cisco Unity and other voice messaging systems. Cisco Unity uses a directory monitor to keep the data in the directory synchronized with the data in the SQL Server 2000 database.

Replicating data to the Domino address book or to Active Directory requires some changes to the directory. If the customer is using:

- Domino, IBM Lotus Domino Unified Communications (DUC) for Cisco must be installed on the Domino servers that will home Cisco Unity subscribers. This adds elements to the address book. In addition, DUC for Cisco must be installed on the client workstation for each Cisco Unity subscriber, which adds elements to the mail file for the client.
- Exchange, the Active Directory schema must be extended with a few Cisco Unity–specific attributes. For information about the Active Directory schema extensions, see the applicable *Cisco Unity Data and the Directory* white paper at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

Enabling Cisco Unity Servers to Communicate with One Another

When two or more Cisco Unity servers are added to the same Domino address book or Active Directory forest, each Cisco Unity server serves a distinct group of subscribers. You can optionally configure the Cisco Unity servers to communicate with one another, which lets you administer subscriber accounts on all Cisco Unity servers from a single location and lets callers leave messages for any subscriber, regardless of the Cisco Unity server with which the subscriber is associated.

If you configure multiple Cisco Unity servers to communicate with one another, two types of Cisco Unity data are stored in the directory:

- A primary location object for each Cisco Unity server. This unique identifier contains the addressing information that Cisco Unity needs to route messages to other Cisco Unity servers. The directory contains one primary location object for each Cisco Unity server in the Domino domain or Active Directory forest.
- Selected subscriber data. The stored properties include the Cisco Unity server with which each subscriber is associated, the subscriber extension, and a recording of the subscriber name.

The directory replicates the information to all Domino servers in the domain (for Domino) or domain controllers and global catalog servers in the forest (for Exchange), which ensures that Cisco Unity has the required access to information.

For detailed information on adding two or more Cisco Unity servers to the same Domino domain or Active Directory forest, see the *Networking Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Enabling Communication (Interoperability) Between Cisco Unity and Other Voice Messaging Systems

Cisco Unity supports several methods for allowing communication between Cisco Unity and other voice messaging systems:

- VPIM (Voice Profile for Internet Mail) is a digital protocol for transferring voice messages between different voice messaging system. To send and receive voice messages by using VPIM, the customer creates a delivery location object for each remote voice messaging system. The third-party voice messaging server must adhere to the VPIM v2 protocol.

  As with the primary location objects, which allow one Cisco Unity server to send messages to subscribers who are associated with another Cisco Unity server, delivery location objects contain the information necessary for Cisco Unity subscribers to exchange voice messages with people who are using another voice messaging system.

- The Audio Messaging Interchange Specification analog (AMIS-a) protocol provides an analog mechanism for transferring voice messages between different voice messaging systems. To send and receive voice messages by using AMIS, the customer creates a delivery location object for each remote voice messaging system.

- The Cisco Unity Bridge acts as a networking gateway between Cisco Unity servers and Octel servers. The Bridge communicates with Octel servers by using the OctelNet analog protocol; it communicates with Cisco Unity servers by using the Digital Networking protocol, which is based on the VPIM protocol, with proprietary extensions.

  Because the servers use different protocols, the Bridge uses nodes to translate messages as appropriate for each server. For the Octel node, the Cisco Unity Bridge maintains a table that contains the Octel server name, unique serial number, and phone number. For the Cisco Unity node, the Bridge maintains another table that contains the Cisco Unity server name, assigned serial number, and domain name. By using these two tables, the Cisco Unity Bridge server can, for example, receive a message from an Octel node, look up the routing information from the Cisco Unity node table, reformat the information for the destination Cisco Unity node, and then send the message to the Cisco Unity node.

For more information on how Cisco Unity works with other voice messaging systems, see the *Networking Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Data That Appears in Both the SQL Server 2000 Database and in the Address Book/Directory Is Automatically Synchronized

Some Cisco Unity information is stored in both the SQL Server 2000 database and in the address book/directory. This data can be changed both from within Cisco Unity (for example, subscriber information can be changed by using the Cisco Unity Administrator), and from outside Cisco Unity (for example, subscriber information can be changed by using Active Directory Users and Computers).

Because this information can be stored and changed in multiple locations, it must be regularly synchronized. Cisco Unity includes separate directory monitors for Domino and for Active Directory that keep the directory synchronized with the SQL Server 2000 database. Every few minutes, the directory monitor checks for new, changed, and deleted objects, and replicates the information.

When two or more Cisco Unity servers are added to the same Active Directory forest, a global catalog monitor keeps the SQL Server 2000 database synchronized with the global catalog. This is how each Cisco Unity server gathers information on subscribers who are associated with other Cisco Unity servers.

Because the amount of data stored in the directory is so small, the impact of replication between the SQL Server 2000 database and the directory is minimal (except when the first Cisco Unity subscribers are created by importing them in bulk from Exchange or from a text file).

Messages from Outside Callers Are Temporarily Stored on the Cisco Unity Server

All messages from outside callers are temporarily stored on the Cisco Unity server before they are forwarded to Domino or Exchange for storage in the subscriber mailbox. This allows Cisco Unity to continue functioning when the network connection between the Cisco Unity server and the Domino or Exchange servers is down, or when one or more Domino or Exchange servers are down.

While Domino, Exchange, and/or the network is offline, Cisco Unity can still answer calls, allow outside callers to look up subscriber extensions, and record voice messages. During this time, subscribers who check their voice messages hear the Unity Messaging Repository (UMR) conversation, which explains that their Domino or Exchange server is not available, but lets them access voice messages left after the problem started. When the Domino server, Exchange server, and/or the network is back on line, the voice messages that were stored in the UMR are routed to the subscriber mailboxes. (In some cases when a network connection or a Domino or Exchange server is down, subscriber-to-subscriber messages are also treated as outside caller messages and stored on the Cisco Unity server until they can be delivered to the appropriate mailbox.)

Some Subscriber Information and Configuration Settings Are Stored on the Cisco Unity Server

Selected recordings and configuration settings are stored in files on the Cisco Unity server, including subscriber greetings (“Hi, this is Pat and I am out of the office today...”), recorded voice names, and some phone system integration settings.

Some Configuration Settings Are Stored in the Registry

Selected server-specific configuration settings are stored in the Windows registry, including some phone system integration and logging settings.

CHAPTER 3

Network Infrastructure Requirements

See the following sections:

- Availability of Network Resources, page 3-1
- Using Firewalls with Cisco Unity, page 3-3
- Sizing and Scaling Cisco Unity Servers, page 3-3
- Audio Codecs, page 3-5

Availability of Network Resources

The following network resources must be available at all times and in close physical proximity to Cisco Unity (over a local area network, not a wide area network), or Cisco Unity functionality will be impaired:

- All name resolution hosts used by standard Windows networks, including DNS hosts. See the "Name Resolution" section on page 3-1.
- Domain controllers that provide authentication for the Cisco Unity service accounts. Windows global catalog servers are also necessary if Cisco Unity services Exchange. See the "Domain Controller Access and Availability" section on page 3-2.
- Message store servers. Each message store server on which Cisco Unity subscribers are homed must be accessible to Cisco Unity. See the "Availability of Message Store Servers" section on page 3-2.
- Active Directory or the Domino directory. See the applicable chapter in this guide:
  - Designing a Cisco Unity System with Exchange as the Message Store
  - Designing a Cisco Unity System with Domino as the Message Store

Name Resolution

Cisco Unity must be able to find the servers it interacts with by resolving the names of those servers to IP addresses, unless the Cisco Unity server is not connected with the network. For example, Cisco Unity can send messages from outside callers to the message store server on which the mailbox of the recipient is homed only if Cisco Unity can find that message store server. Name resolution is also used when:

- A subscriber uses the Cisco Unity telephone user interface (TUI) to listen to messages or send messages to other subscribers. Name resolution is used by Cisco Unity whenever a process requires the Unity application to execute commands that leave the Cisco Unity server and access information across the network to the mailbox stores where subscriber mailboxes are located.

- Administrators access the Cisco Unity Administrator from other servers, which is primarily done when using the administrative web interfaces. Typically, if a server name is used instead of an IP address, the server name must be resolved to an IP address before access can occur over the network.
- Subscribers access the Cisco Unity Assistant or the Cisco Unity Inbox. Typically, if a server name is used instead of an IP address, the server name must be resolved to an IP address before access can occur over the network.

The Cisco Unity server must use Dynamic DNS (DDNS) or another version of DNS that supports dynamic updates as described on the Microsoft website. Simply creating a host file on the Cisco Unity server is not sufficient.

When Domino is the message store, note the following:

- If Notes clients are using Notes Name Resolution, Cisco Unity must also use Notes Name Resolution through the Notes client that is installed on the Cisco Unity server. DDNS is required on the Windows domain controller in the domain to which the Cisco Unity server belongs.
- You can install the Windows DNS service on the Cisco Unity server in either a Unified Messaging or a Voice Messaging configuration. With Domino, the Cisco Unity server is configured as a Windows domain controller to service Domino Notes clients via DUC. This is a Cisco Unity requirement, not a DUC requirement. The Cisco Unity server supports its own dedicated domain for Domino.

When Exchange is the message store, note the following:

- The DDNS server must be accessible by Cisco Unity and the supporting Exchange servers.
- In a Voice Messaging configuration with failover, install the Windows DNS service on the Cisco Unity secondary failover server or on a dedicated DC/GC server.
- In a Voice Messaging configuration without failover, when the Cisco Unity server is a Windows domain controller and all other servers in the domain are Exchange servers that are used only to support Cisco Unity, install the Windows DNS service on the Cisco Unity server. In this configuration, the Cisco Unity server supports its own dedicated domain for Exchange.
- In a Unified Messaging configuration when Exchange is the message store, do not install the Windows DNS service on the Cisco Unity server.

Domain Controller Access and Availability

For all configurations and all message stores, Cisco Unity must have access to a Windows domain controller to authenticate service accounts and, when Exchange is the message store, to authenticate subscribers.

When Domino is the message store, subscribers can be authenticated for GUI-based access to Cisco Unity by using either Windows authentication or Domino authentication; Domino authentication does not require access to a Windows domain controller.

Availability of Message Store Servers

When Cisco Unity is installed, the installer specifies one Domino or Exchange server that Cisco Unity connects with; this is known as the partner Domino server or the partner Exchange server. The partner server is the home of the Cisco Unity system mailbox (alias: Unity_<ServerName>. The Unity system mailbox is the mailbox that originates voice messages from outside callers. The partner server is also the home for default mailboxes and distribution groups (Cisco Unity distribution lists) that are created

during installation. If Cisco Unity subscribers are homed on servers other than the partner Exchange server or the Domino mail drop server, all voice messages from outside callers pass through the partner server or the mail drop server on their way to the home servers for Cisco Unity subscribers.

When the partner Exchange server, the mail drop Domino server, or a message store server on which Cisco Unity subscribers are homed is unavailable, Cisco Unity functionality is affected in the following ways:

- Messages from outside callers are stored on the Cisco Unity server in the Unity Message Repository (UMR), and can be retrieved during the outage. However, voice messages that were previously received by subscribers are not available until the home server is back online.
- When the home server of a calling subscriber is down, any messages from that subscriber are stored on the Cisco Unity server in the UMR, and can be retrieved by the recipient during the outage.
- Message waiting indicators and message notification will not work.

Tip Make sure that the importance of message store availability is clearly understood prior to installing one or more Cisco Unity servers, particularly those that service message stores on separate servers.

Using Firewalls with Cisco Unity

Revised May 6, 2008

Cisco Unity can coexist with firewalls. However, note that Cisco Unity should never be deployed outside of a firewall. Doing so can expose the Cisco Unity server to unwanted intrusion from the Internet, even if the server is hardened.

For detailed firewall requirements, see the following sections in the *System Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html:

- "Network Requirements"
- "Failover Requirements for Separating Cisco Unity Servers by a Firewall"
- "Standby Redundancy Requirements for Separating Cisco Unity Servers by a Firewall"

Sizing and Scaling Cisco Unity Servers

When sizing a Cisco Unity server, follow these guidelines:

- Maximum Number of Users on Dedicated Domino or Exchange Servers, page 3-4
- Storage Capacity for Voice Messages, page 3-4
- Number of Voice Ports, page 3-4

For a list of servers that meet Cisco Unity specifications, see the *Cisco Unity Supported Platforms List* at http://cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.

Maximum Number of Users on Dedicated Domino or Exchange Servers

You should not allow the Domino or Exchange servers to service the maximum number of Domino or Exchange users that IBM Lotus or Microsoft allow. In addition, servers qualified by Cisco as Exchange message store servers for use with Cisco Unity have a maximum number of Exchange users, and the customer should not allow the number of users on these servers to reach the maximum.

You should also be careful not to exceed the disk capacity for the information store. For example, in order to enable recovery if the information store is corrupted, Microsoft recommends that the total size of an Exchange information store never exceed 50 percent of the capacity of the drive on which the information store is installed. For more information, see the Microsoft website.

Storage Capacity for Voice Messages

For Cisco Unity systems that are configured for Voice Messaging, base the server requirements on the total number of voice storage minutes required for each subscriber. A supported Cisco Unity server generally provides storage for 20 to 30 minutes of voice messages per subscriber for the maximum number of subscribers supported on that server.

For Cisco Unity systems that are configured for Unified Messaging, it is not possible to base server requirements on the total number of voice storage minutes required for each subscriber, because the message store also includes e-mail messages and possibly faxes. However, you can calculate the storage requirement for the desired number of voice storage minutes and add that to the current mailbox limits.

If the customer is replacing an existing voice messaging system with Cisco Unity, it may be possible to obtain information from the existing system on the average number of minutes of voice messages that subscribers currently have. You can then multiply the average number of minutes by the recording size per minute—according to the codec that Cisco Unity will use to record messages—to arrive at the average amount of disk space required for voice messages per subscriber.

Start with a one-to-one correlation of legacy voice messaging system to Cisco Unity. If the legacy system handles a larger capacity than the largest Cisco Unity server, consider splitting the legacy subscriber population onto more than one Cisco Unity server by extension number ranges or prefixes. It is not necessary to segment subscribers onto backend message stores by extension number ranges or prefixes but it may be easier to manage.

For more information, see the "How Codecs Affect the File Size of Voice Messages" section on page 3-5.

Number of Voice Ports

To determine the number and configuration of voice ports required, you can start with the existing voice messaging system, if applicable. This may give you some idea how many ports are required for taking voice messages, for turning message waiting indicators on and off, and for message notification.

In a Unified Messaging configuration, Cisco Unity uses telephone record and playback (TRAP), to allow subscribers who use Notes or Outlook for voice messaging to play and record voice messages over the phone rather than by using speakers and a microphone. This feature is especially desirable when subscribers work in cubicles, where there is a lack of privacy. However, when a subscriber plays or records a message by using TRAP, a port on the Cisco Unity server is used. (No port is used when a subscriber uses speakers and a microphone to play and record messages.) If the customer wants subscribers to use TRAP, calculations for the total number of voice ports required will need to take this into account.

For Cisco Unity failover, the primary and secondary servers must have the same number of ports.

In some cases you might find that an existing voice messaging system has more ports than the current maximum number of voice ports on a Cisco Unity system. In this case, the customer can purchase additional Cisco Unity servers and connect them by using Cisco Unity Digital Networking.

Audio Codecs

An audio codec is an algorithm that encodes and decodes (and compresses or decompresses) audio data. Cisco Unity uses audio codecs with streaming (live conversation) and for WAV-file voice messages. Cisco Unity supports the following audio codecs:

- G.711 Mu-Law (the default codec)
- G.711 A-Law
- G.729a
- Intel Dialogic OKI ADPCM 8 kHz
- Intel Dialogic OKI ADPCM 6 kHz
- GSM 6.10
- G.726 codec (supported only when using VPIM to communicate with another voice-messaging system)

In general, choose an audio codec based on available storage capacity for voice messages and on available network bandwidth. We recommend using G.711 whenever possible because of its excellent quality for recording and playback. However, if other considerations prevent the customer from using G.711, it is fine to use G.729a, which is also a voice-quality codec. (A large-scale or multiserver deployment may require the use of more than one codec.)

The rest of this section discusses some of the issues to consider when choosing a codec. For a more thorough analysis, see the *Audio Codecs and Cisco Unity* white paper at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

For information on how codec choice affects Active Directory, see the applicable *Active Directory Capacity Planning* white paper at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

How Codecs Affect the File Size of Voice Messages

Stored voice messages can consume considerable amounts of disk space. The amount of storage a WAV file uses depends on what kind of compression the codec uses, if any. The higher the compression, the smaller the file and the smaller the disk-space impact on the database and at the subscriber workstation. However, some sound-quality reduction and some CPU processing overhead may result when compressing messages during recording and decompressing at playback.

As illustrated in Table 3-1, voice messages that are recorded in G.711 Mu-Law and A-Law require the most disk space to store, while G.729a offers the smallest file size.

Note Audio quality ratings are subjective, and are provided here only for basic comparison between the different fully supported codecs.

Table 3-1 Voice Message File Sizes and Audio Quality Ratings

Audio Codec	Approximate File Size, 1-Minute Message	Quality Rating
G.711 Mu-Law and A-Law	480 KB	Excellent
G.726 32 Kbps	240 KB	Fine
OKI ADPCM 8 kHz	240 KB	Fine
OKI ADPCM 6 kHz	180 KB	Fine
GSM 6.10	98 KB	Good
G.729a	60 KB	Good

TTS, TTY, Pocket PCs, and Hand-Held Computers

For Cisco Unity sites using Text to Speech (TTS), any supported codec can be used to record messages. However, TTS output is currently available only in G.711 and G.729a audio formats.

For Cisco Unity sites using TTY, G.711 is required. The TTY standard does not support other codecs.

GSM 6.10 is supported for playback on a Pocket PC, and is a higher quality recording format than MP3. G.711 and G.729a usually are not compatible with hand-held computers.

Interoperability Among Multiple Voice-Messaging Systems

If multiple Cisco Unity servers will communicate with one another via Cisco Unity Digital Networking or VPIM, or if Cisco Unity will communicate with other voice-messaging systems by using AMIS, the Cisco Unity Bridge, or VPIM, you must choose a compatible codec. Table 3-2 shows a summary of codec considerations for Cisco Unity networking options.

Table 3-2 Networking Interoperability Comparison for Audio Codecs

Networking Option	Supported Codecs
AMIS	The AMIS protocol is not dependent on audio format. The Cisco Unity servers can use any of the supported codecs.
Cisco Unity Bridge	Octel Analog Networking is not dependent on audio format. The Cisco Unity servers must use either G.711 or G.729a in order to communicate with the Cisco Unity Bridge servers.
VPIM	For inbound messages, Cisco Unity can convert voice messages to any codec that Cisco Unity supports. For outbound voice messages, Cisco Unity can either convert voice messages to G.726 format or not convert at all. Not converting is useful when you are using VPIM to send voice messages between Cisco Unity servers.

CHAPTER 4

Designing a Cisco Unity System with Exchange as the Message Store

This chapter focuses on using Exchange as the message store and Active Directory as the directory for Cisco Unity. All references to Exchange apply to the currently supported versions of Exchange—Exchange 2007 and Exchange 2003—unless specified otherwise. Exchange 2000 is supported only for upgrades from Cisco Unity 4.x and is, therefore, not discussed in this design guide.

See the following topics:

- Deployment Models, page 4-1
- Physical Placement and Network Infrastructure, page 4-4
- Considerations for Customer-Provided Infrastructure, page 4-5
- Considerations for Cisco-Provided, Dedicated Infrastructure, page 4-9

Deployment Models

You can deploy Cisco Unity by using customer-provided infrastructure or by using dedicated, Cisco-provided infrastructure.

With customer-provided infrastructure, Cisco Unity can be configured either as Unified Messaging or as Voice Messaging. Cisco Unity is a part of the messaging environment, it services subscribers who are homed on existing Exchange e-mail servers, and it uses existing DC/GCs. For more information, see the following sections:

- Unified Messaging with Customer-Provided Infrastructure, page 4-2
- Mixed Unified Messaging and Voice Messaging with Customer-Provided Infrastructure, page 4-2
- Voice Messaging with Customer-Provided Infrastructure, page 4-3

With dedicated, Cisco-provided infrastructure, Cisco Unity is configured as Voice Messaging. Each Cisco Unity subscriber requires a separate Active Directory user account in a dedicated forest and a separate Exchange mailbox that holds only Cisco Unity voice messages on a separate, dedicated Exchange server that homes only Cisco Unity voice messages. For more information, see the "Voice Messaging with Cisco-Provided, Dedicated Infrastructure" section on page 4-2.

If the customer has more than one data center, you can combine deployment models. For more information, see the "Multi-Site WAN with Distributed Messaging" section on page 4-3.

Unified Messaging with Customer-Provided Infrastructure

Revised May 6, 2008

For the Cisco Unity Unified Messaging configurations, Cisco Unity installs into an existing infrastructure, is a part of the messaging environment, services subscribers who are homed on existing Exchange e-mail servers, and uses existing DC/GCs. This reduces administrative overhead when compared with maintaining a Cisco Unity Voice Messaging solution or maintaining a legacy voice messaging system. With Unified Messaging, only one messaging infrastructure is required to support both e-mail and voice messaging. The customer is responsible for maintaining the DC/GCs, Exchange servers, and DNS.

Each Cisco Unity server can be connected to a circuit-switched phone system, to Cisco Unified Communications Manager, or to both. If the phone system has ports available, you can connect more than one Cisco Unity server to each phone system.

When you are setting up two or more Cisco Unity servers in the same Active Directory forest, the Cisco Unity servers can be networked by using Cisco Unity Digital Networking.

Mixed Unified Messaging and Voice Messaging with Customer-Provided Infrastructure

When mixing Unified Messaging and Voice Messaging deployment models, the Unified Messaging portion of the deployment is the same as a Unified Messaging deployment without the Voice Messaging subscribers.

The Voice Messaging subscribers require separate accounts and mailboxes:

- Each Voice Messaging subscriber requires a separate Active Directory user account in the existing forest.
- Each Voice Messaging subscriber requires a separate Exchange mailbox that holds only Cisco Unity voice messages. The mailbox can be stored on existing Exchange servers or can be stored on separate, dedicated Exchange servers that home only Cisco Unity voice messages. If the mailboxes are stored on existing Exchange servers, the customer is responsible for support for the servers. If the mailboxes are stored on Exchange servers that are dedicated to Cisco Unity voice messages, Cisco will support the Exchange servers.

  If the Voice Messaging subscribers are homed on one or more dedicated Exchange servers on which the Voice Mail Run-time Edition of Microsoft Exchange was installed, those subscribers do not need Microsoft Client Access Licenses (CALs). Unified Messaging subscribers all need CALs.

For more information on the Unified Messaging portion of a mixed system, see the "Unified Messaging with Customer-Provided Infrastructure" section on page 4-2.

For more information on the Voice Messaging portion of a mixed system, see the "Voice Messaging with Customer-Provided Infrastructure" section on page 4-3.

Voice Messaging with Cisco-Provided, Dedicated Infrastructure

Revised May 6, 2008

In this deployment model:

- Each Voice Messaging subscriber requires a separate Active Directory user account in a dedicated forest.

- Each Voice Messaging subscriber requires a separate Exchange mailbox that holds only Cisco Unity voice messages on a separate, dedicated Exchange server that homes only Cisco Unity voice messages.

The advantages of this model include the following:

- The customer does not need to extend the Active Directory schema in the existing forest.
- Some companies have one department that manages the phone and voice-messaging system and a separate department that manages Exchange. Dedicated Exchange servers for Cisco Unity voice messages may simplify implementation and maintenance.
- Some customers like to keep voice messages and e-mail messages separate.
- If Active Directory accounts are created in an existing forest and mailboxes are stored on existing Exchange servers, the customer is responsible for support for the servers. If accounts are created in a dedicated forest and mailboxes are stored on Exchange servers that are dedicated to Cisco Unity voice messages, Cisco will support the entire Cisco Unity system, including dedicated DC/GCs (if any) and dedicated Exchange servers.

The disadvantages of this model include:

- A more complicated and time-consuming migration to a Unified Messaging configuration.
- More overhead for maintaining the Active Directory and Exchange infrastructure.
- Possible additional hardware expense.

Voice Messaging with Customer-Provided Infrastructure

Revised May 6, 2008

In this deployment model:

- Each Voice Messaging subscriber requires a separate Active Directory user account in the existing forest. The customer can create a separate domain for these accounts, but that is not required.
- Each Voice Messaging subscriber requires a separate Exchange mailbox that holds only Cisco Unity voice messages. The mailbox can be stored on existing Exchange servers or can be stored on separate, dedicated Exchange servers that home only Cisco Unity voice messages. If the mailboxes are stored on existing Exchange servers, the customer is responsible for support for the servers. If the mailboxes are stored on Exchange servers that are dedicated to Cisco Unity voice messages, Cisco will support the Exchange servers.

This model has the following advantages:

- It simplifies the migration from a Voice Messaging Configuration to a Unified Messaging configuration.
- Some companies have one department that manages the phone and voice-messaging system and a separate department that manages Exchange. If the two departments do not communicate with one another, dedicated Exchange servers for Cisco Unity voice messages may simplify implementation and maintenance.

Multi-Site WAN with Distributed Messaging

When deploying Cisco Unity in a multi-site WAN with distributed messaging, the customer uses two or more of the deployment models discussed earlier in this section, either at the same physical site or in geographically diverse data centers connected by a WAN. In this deployment, network bandwidth should meet the minimum Microsoft Exchange server inter-site requirements.

When all Cisco Unity servers will be in the same Active Directory forest and the customer wants subscribers to be able to send voice messages across servers, use Cisco Unity Digital Networking to connect them. The messaging functionality across Cisco Unity servers is the same as the messaging functionality on a single Cisco Unity server.

When Cisco Unity servers will be in two or more Active Directory forests, you can use VPIM networking to connect them. The messaging functionality across Cisco Unity servers is not identical to the messaging functionality on a single Cisco Unity server, but most functionality is preserved. (VPIM networking requires that the Cisco Unity Voice Connector for Microsoft Exchange be installed on an Exchange 2003 or Exchange 2000 server in each forest.) For more information, see the applicable *Networking Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

When the customer wants Cisco Unity to communicate with another voice messaging system, the method you use to network them and the functionality that is available depend on the voice-messaging system. For example, to network Cisco Unity with Cisco Unity Express or with Cisco Unity Connection, you use VPIM networking, and to network Cisco Unity with Octel voice-messaging systems, you use the Cisco Unity Bridge. For more information, see:

- The applicable *Networking Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
- *Networking Options Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Physical Placement and Network Infrastructure

Revised May 6, 2008

To ensure that Cisco Unity functions properly, we require that a Cisco Unity server be in the same data center as the following servers:

- The Exchange server that Cisco Unity communicates with, commonly known as the partner Exchange server. For more information on the partner Exchange server, see the "Exchange Considerations (All Versions)" section on page 4-7.
- Every Exchange server on which mailboxes for that Cisco Unity server are homed. If Cisco Unity is separated by a WAN from an Exchange server on which subscriber mailboxes are homed, a second Cisco Unity server must be co-located with the remote Exchange server.
- At least one domain controller. If Cisco Unity subscribers are homed in more than one domain, a DC for each domain must be in the same data center as the Cisco Unity server.
- At least one global catalog server.
- At least one DNS server.

These requirements apply regardless of whether the non-Cisco Unity servers are customer provided, or are Cisco provided and dedicated to Cisco Unity.

Connect the Cisco Unity server and the servers that Cisco Unity relies on with a high-speed switched gigabit network with no congestion. Total MAPI response time must be less that 10 milliseconds.

The Cisco Unity server should be installed into the same Windows site as the Exchange servers it services.

Note the following:

- Cisco Unity can coexist with firewalls. However, note that Cisco Unity should never be deployed outside of a firewall. Doing so can expose the Cisco Unity server to unwanted intrusion from the Internet, even if the server is hardened.

For detailed firewall requirements, see the following sections in the *System Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html:

  - "Network Requirements"
  - "Failover Requirements for Separating Cisco Unity Servers by a Firewall"
  - "Standby Redundancy Requirements for Separating Cisco Unity Servers by a Firewall"

- When Cisco Unity is remotely connected with an IP phone system, it is acceptable to calculate the per-port bandwidth and necessary overhead. The aggregate total of bandwidth for all ports plus any necessary overhead is the minimum bandwidth required.
- Cisco Unity supports a maximum of 250 Exchange information stores.
- If the Cisco Unity server has two NICs, the NICs cannot be used for load balancing. If dual NICs are configured, we recommend that they be configured in adaptive fault tolerant (AFT) or network fault tolerant (NFT) mode. For additional information about dual NICs, see the "Customizing the Cisco Unity Platform" chapter in the applicable Cisco Unity installation guide, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
- In general, Cisco Unity failover servers can be on separate network segments or subnets. However, both servers must reside in the same Windows site, and each server must directly connect to the DCs, GCs, message store servers, and other network resources necessary to operate normally. For requirements for failover over a WAN, see the "Requirements for Cisco Unity Failover Over a WAN" section in the *System Requirements for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
- For information on network requirements for phone system integrations, see the "Integrating Cisco Unity with the Phone System" chapter.

Considerations for Customer-Provided Infrastructure

See the following sections:

- Active Directory Considerations, page 4-5
- Exchange Considerations (All Versions), page 4-7
- Exchange Considerations That Apply Only Exchange 2007, page 4-8

Active Directory Considerations

Note the following Active Directory considerations when a Cisco Unity implementation will use customer-provided Active Directory infrastructure:

- The Active Directory schema must be extended for Cisco Unity to function properly. For information on capacity planning recommendations related to using Cisco Unity with Active Directory, see the *Active Directory Capacity Planning (Cisco Unity Version 5.x and Later with Microsoft Exchange)* white paper at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html. This white paper also includes sizing information for Active Directory objects that have been voice enabled by Cisco Unity. Finally, it discusses the Cisco Unity schema: what is required when the customer extends the schema, and when it is required.

For general information on Cisco Unity and Active Directory, see the applicable *Cisco Unity Data and the Directory* white paper, also at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

- The main Cisco Unity services log on by using two Active Directory accounts that the installer creates during Cisco Unity installation:
  - Message store services log on by using the message store services account. These services send and receive messages on behalf of the subscriber. The account with which these services log on must have direct access to the Exchange message store where the subscribers reside.
  - Directory services log on by using the directory services account. These services write to user, group, and contact objects when the objects are imported into Cisco Unity, and they write to individual subscriber properties when a subscriber or an administrator changes personal settings for the subscriber.

  Each service account can be used by more than one Cisco Unity server in the same domain.
- The Cisco Unity installation, message store services, and directory services accounts require Active Directory permissions to create objects during installation and to manage the objects during regular operation. The Cisco Unity Permissions wizard grants the required permissions automatically based on options the installer chooses for the customer configuration. For a detailed explanation of the permissions required, see the Help file *Permissions Granted by the Cisco Unity 5.0(1)+ Permissions Wizard* at http://ciscounitytools.com/HelpFiles/PW501/PWHelpPermissionsSet_ENU.htm.

  The installation and directory services accounts also require Exchange permissions. For more information, see the Help file *Delegating Exchange Administrative Control for Cisco Unity 5.0(1)+* at http://ciscounitytools.com/HelpFiles/PW501/PWHelpExchange_ENU.htm.

  For additional information on the Permissions wizard, see the Help file *Granting Permissions with Cisco Unity 5.0(1)+ Permissions Wizard* at http://ciscounitytools.com/HelpFiles/PW501/PWHelp_ENU.htm.
- The Cisco Unity directory service periodically queries the local DC and GC for changes to Active Directory data that also appears in the SQL Server database on the Cisco Unity server. If any changes are found, the directory service updates the SQL Server or MSDE database accordingly. These queries do not significantly affect the performance of the DC or GC unless a significant number of changes have been made to Active Directory user accounts.
- Cisco Unity is an Active Directory site-aware application. If Active Directory sites are configured correctly, when Cisco Unity queries Active Directory for directory updates, a DC or GC in the site will respond rather than a DC or GC in a remote site. In a Unified Messaging configuration, in which Active Directory sites are already configured, this should not be an issue. For large Voice Messaging configurations, with Cisco Unity servers in multiple separate locations in a dedicated Active Directory forest, Active Directory sites must be configured to respond intelligently to queries.
- Active Directory Application Mode (ADAM) is not supported.

Exchange Considerations (All Versions)

Note the following Exchange considerations when a Cisco Unity implementation will use customer-provided Exchange infrastructure:

- When Cisco Unity is installed, the installer chooses a partner Exchange server, which is the home of several default Cisco Unity mailboxes, including:
  - The Cisco Unity system mailbox (alias: Unity_<ServerName>), which is the mailbox that originates voice messages from outside callers. (Voice messages from Cisco Unity subscribers originate from the mailbox of the caller.) Each Cisco Unity server must have its own system mailbox.
  - The mailbox from which broadcast messages are sent.
  - If Cisco Unity is interoperating with other voice messaging systems, the mailboxes that send voice messages to and receiver voice messages from the other voice messaging systems.

  The partner Exchange server can be running Exchange 2007, Exchange 2003, or Exchange 2000, and it can be either a clustered or non-clustered Exchange server.

  Because of the importance of the partner Exchange server in a Cisco Unity installation, the server should be selected primarily on the basis of availability and secondarily on the basis of performance.
- Exchange performance is critical to Cisco Unity performance. To ensure that Exchange performance will not adversely affect Cisco Unity, we recommend that customers assess the performance of their Exchange infrastructure before installing Cisco Unity. For example, the Microsoft TechNet article *Exchange Server 2003: Ruling Out Disk-Bound Problems* (http://technet.microsoft.com/en-us/library/aa997558.aspx) can provide useful guidance.
- Exchange servers must meet Microsoft requirements, including the maximum number of users per server, the proper amount of memory, the proper processors and processor speed, hard disks that can meet disk-access response times, and placement of data files and transaction log files.

  Cisco Unity cannot support Exchange servers that have performance bottlenecks such as slow hard drives or insufficient memory. For example, if slow hard drives or the lack of a dedicated mirror for transaction logs cause delays in recording log transactions, MAPI access (which is used by Microsoft Outlook, Exchange, and Cisco Unity to access Exchange) will be temporarily suspended until the transaction buffers can be cleared to a certain level. This can substantially delay phone access to Cisco Unity.
- The Cisco Unity Voice Connector for Microsoft Exchange, which is required for communicating with another voice-messaging system by using AMIS, the Cisco Unity Bridge, or VPIM, must be installed on the partner Exchange server. The Voice Connector can also, optionally, be installed on one or more other Exchange 2000 or Exchange 2003 servers to optimize message routing via Exchange's native, cost-based routing. (The Voice Connector cannot be installed on an Exchange 2007 server.)
- For information on the impact of audio codecs on Exchange, see the "Audio Codecs" section on page 3-5.
- In a Voice Messaging configuration, to prevent the message store from filling the hard disk, some customers configure storage limits in Exchange, and use Cisco Unity Message Store Manager to delete old messages. For example, messages older than 30 days might be moved to the deleted-messages folder, and messages older than 60 days might be purged. For more information on Message Store Manager, see the Message Store Manager Help at http://ciscounitytools.com/HelpFiles/MSM/MSMConsoleHelp_ENU.htm.

- In a Voice Messaging configuration, to help prevent Exchange transaction logs from filling the hard disk, a wizard in Cisco Unity Setup prompts the installer to change the circular-logging setting for any message store in the forest for which circular logging is turned off. If the customer is using an Exchange-aware backup application to back up Exchange message stores and clear transaction logs, the installer can choose not to change the circular-logging setting.

Exchange Considerations That Apply Only Exchange 2007

Note the following Exchange 2007 considerations when a Cisco Unity implementation will use customer-provided Exchange 2007 infrastructure:

- Exchange 2007 is supported as the message store only when Cisco Unity is configured as Unified Messaging.
- The Cisco Unity Voice Connector for Microsoft Exchange, which is required for communicating with another voice-messaging system by using AMIS, the Cisco Unity Bridge, or VPIM, can only be installed on an Exchange 2000 or an Exchange 2003 server. A Voice Connector is not currently available for Exchange 2007. If the customer has already configured a pure Exchange 2007 environment, an Exchange 2000 or Exchange 2003 server cannot be added to the environment and, therefore, Cisco Unity functionality that requires the Voice Connector is not available.
- Cisco Unity Mobile Message Access for BlackBerry is not supported for Exchange 2007.
- Integrated messaging via IMAP with Exchange 2007 is supported when Cisco Unity voice messages are stored in Exchange 2000 or Exchange 2003.

  With Exchange 2000 or Exchange 2003, you can store e-mail messages in one Exchange message store, store Cisco Unity voice messages in another message store, and view both types of messages in a Microsoft Outlook Inbox. In this configuration, known as integrated messaging, you:

  - Configure Outlook to use MAPI to communicate with the message store that contains e-mail (MAPI is required because the e-mail message store commonly also contains calendars and contacts).
  - Configure Outlook to use IMAP to communicate with the message store that contains Cisco Unity voice messages. (Outlook only supports one MAPI connection at a time.)
  - Enable Exchange rich-text format on Exchange servers, which converts IMAP to TNEF-encoded IMAP. (If you do not enable rich-text format, voice messages appear in the Outlook Inbox as e-mail messages, so ViewMail for Outlook is not available.)

  Exchange 2007 does not support TNEF-encoded IMAP, but you can still use an integrated messaging configuration with Exchange 2007 if you store e-mail in Exchange 2007 and store Cisco Unity voice messages in Exchange 2000 or Exchange 2003.

For more information on Cisco Unity limitations when Exchange 2007 is the message store, see the subsection “Cisco Unity with Exchange: Exchange Server 2007” in the section “New and Changed Requirements and Support—Release 5.0(1)” in *Release Notes for Cisco Unity Release 5.0(1)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Considerations for Cisco-Provided, Dedicated Infrastructure

Note the following considerations when a Cisco Unity implementation will use Cisco-provided, dedicated Exchange and Active Directory infrastructure:

- Ensure that the servers selected for Cisco Unity and for Exchange are able to handle the proposed number of users. For information on selecting servers, see the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.
- If the customer is installing Cisco Unity and Exchange servers in multiple locations and if they will all be in the same Active Directory forest, ensure that Active Directory sites are configured.
- If two or more Cisco Unity servers are being installed in a forest but they are being installed in different forest roots, configure a one-way trust to enable client authentication. For more information, see the "Grant Unity Access" section in the *Client Access in a Voice Messaging-Only Deployment (Cisco Unity Version 4.0)* white paper at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

Note The version of GrantUnityAccess shipped with Cisco Unity 5.0 requires a two-way trust due to caveat CSCsi68156. An updated version of GrantUnityAccess that does not have this problem is available on the "4.x/5.x Tools" page on the Cisco Unity Tools website at http://ciscounitytools.com/4_x_tools.htm.

- Within a given data center, if the location will have two Exchange servers, we recommend that the customer make both servers DC/GCs and run DNS on both servers. If the location will have four or more Exchange servers, we recommend that the customer make half of the Exchange servers DC/GCs and run DNS on two of them.
- In a Voice Messaging configuration, to prevent the message store from filling the hard disk, some customers configure storage limits in Exchange, and use Cisco Unity Message Store Manager to delete old messages. For example, messages older than 30 days might be moved to the deleted-messages folder, and messages older than 60 days might be purged. For more information on Message Store Manager, see the Message Store Manager Help at http://ciscounitytools.com/HelpFiles/MSM/MSMConsoleHelp_ENU.htm.
- The Cisco Unity Voice Connector for Microsoft Exchange, which is required for communicating with another voice-messaging system by using AMIS, the Cisco Unity Bridge, or VPIM, must be installed on the partner Exchange server. The Voice Connector can also, optionally, be installed on one or more other Exchange 2000 or Exchange 2003 servers to optimize message routing via Exchange's native, cost-based routing. (The Voice Connector cannot be installed on an Exchange 2007 server.)
- The customer can configure Exchange clustering by using the Voice Mail Run-Time Edition of Microsoft Exchange Server 2003 Enterprise Edition that is shipped with Cisco Unity. However, the customer is responsible for supporting the Exchange cluster and any custom hardware or configuration.
- In a Voice Messaging configuration, to help prevent Exchange transaction logs from filling the hard disk, a wizard in Cisco Unity Setup prompts the installer to change the circular-logging setting for any message store in the forest for which circular logging is turned off. If the customer is using an Exchange-aware backup application to back up Exchange message stores and clear transaction logs, the installer can choose not to change the circular-logging setting.

CHAPTER 5

Designing a Cisco Unity System with Domino as the Message Store

This chapter focuses on using IBM Lotus Domino as the message store and a Domino address book as the directory for Cisco Unity.

See the following sections:

- Overview of Cisco Unity with Domino and Notes, page 5-1
- Cisco Unity and the Domino Address Book, page 5-8
- Unified Messaging Configurations, page 5-9
- Voice Messaging Configuration, page 5-10
- Criteria for a Supported Configuration, page 5-10
- Deploying Cisco Unity for Lotus Domino, page 5-11
- Feature Parity Between Cisco Unity for Domino and Cisco Unity for Exchange, page 5-14

Overview of Cisco Unity with Domino and Notes

This section provides an overview of the characteristics of a Cisco Unity system with Domino as the message store. Unless noted, all information applies to both Unified Messaging and Voice Messaging configurations.

See the following sections:

- Maximum Number of Cisco Unity Subscribers, page 5-2
- Domino Address Book Terminology, page 5-2
- IBM Lotus Domino Unified Communications (DUC) for Cisco on Domino Servers and on Client Workstations, page 5-2
- Address Book Server, Message Store Server, and Mail Drop Server, page 5-4
- Windows Domains and Domino Domains, page 5-5
- Server Placement, page 5-5
- Active Directory Accounts and Permissions, page 5-6
- Authentication, page 5-6
- Domino Permissions, page 5-7
- Cisco Unity Subscribers and Domino Users, page 5-7

- Domino Clusters, page 5-7
- Message Routing, page 5-8
- Notes Client on the Cisco Unity Server, page 5-8
- Client Access Licenses, page 5-8
- Backing Up and Restoring Data, page 5-8
- Migrating from Cisco Unity for Exchange, page 5-8

Maximum Number of Cisco Unity Subscribers

Cisco Unity for Domino deployments are limited to one Cisco Unity server or one pair of failover servers with a maximum of 7,500 subscribers.

Domino Address Book Terminology

Names.nsf is the first address book (directory) file in a Domino domain, and is created when the first Domino server is installed. Each additional Domino server that is added to the Domino domain receives a replica of Names.nsf.

During Cisco Unity installation, the installer specifies a Domino address book on a Domino server. In general, this address book will be a replica of Names.nsf. The customer can create Cisco Unity subscriber accounts by importing user data from the specified address book. Cisco Unity monitors the address book for changes to Domino users who are also Cisco Unity subscribers and to Domino distribution lists.

A secondary address book is an address book that is typically created to house non-local mail users, who do not own a mailbox in the domain or enterprise. (In Domino, the Person documents for these users have “Other Internet Mail” set in the Mail System field.) The Active Directory equivalent is contacts. You can add one additional (secondary) subscriber address book by using the Cisco Unity Administrator. The secondary address book must reside in the same Domino domain as the primary address book, and cannot be a replica of an address book in another Domino domain.

By default, the address book that the installer specifies in the Message Store Configuration wizard during Cisco Unity Setup is monitored for changes to Cisco Unity data. In addition, you can add up to eight monitored address books by using the Cisco Unity Administrator. Monitored address books may be needed when there are multiple Cisco Unity servers that will be set up for Digital Networking. For more information, see the “Managing Monitored Address Books” section in the “Digital Networking” chapter of the *Networking Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

IBM Lotus Domino Unified Communications (DUC) for Cisco on Domino Servers and on Client Workstations

To use Domino as the message store and directory, the customer must install components of IBM Lotus Domino Unified Communications (DUC) for Cisco on Domino servers:

- csServer must be installed on each Domino server that homes Cisco Unity subscribers. If Cisco Unity subscribers are homed on Domino servers in a cluster, csServer must be installed on every Domino server in the cluster.

- csAdmin, the administration component of DUC for Cisco, must be installed on the Domino server that pushes directory information out to the other Domino servers. You install csAdmin only once for the domain.

In addition, DUC for Cisco client software must be installed on the client workstation of each Notes user who will be a Cisco Unity subscriber. Installing the client software adds VCR-style recording and playback controls to the message form, and provides message notification, message waiting indicators, and a Lotus Mail template for recording and playing voice messages.

For information on the versions of the following software currently supported, see the "Domino Requirements—Message Store" section of *System Requirements for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html:

- Domino versions supported on message store servers
- DUC for Cisco versions supported on Domino servers
- Notes versions supported on the Cisco Unity server
- Operating systems supported on Domino servers running DUC for Cisco

Changes That csAdmin Makes to the Domino Address Book

Table 5-1 shows the elements added to the Domino address book when csAdmin is installed. If csAdmin is uninstalled, these items are removed from the address book.

Table 5-1 Elements That csAdmin Adds to the Address Book

Element	Name
Forms	Unity Location
Views	• Unity Locations • ($UnityLocLookup) • ($UnityNameLookup)
Agent	UC License Tracking
Subforms	• $CSUnityDLSubform • $CSUnityUserSubform • $GroupExtensibleSchema • $PersonExtensibleSchema

Changes That csClient Makes to the Mail File

When csClient software is installed on a client workstation, the elements in Table 5-2 are added to the mail file. If csClient is uninstalled, these elements are removed from the mail file.

Table 5-2 Elements That csClient Adds to the Mail File

Element	Name
Forms	• UCDisplayInfo • Voice Message • (Display Received Voice Message) • (UCMemo)
Views	• Voice Inbox • ($UCInbox)—this view is added when the user is imported into Cisco Unity
Agents	• (UCEnable) • (UCPreferences)
Images	• Phone.jpg • act_EDIT.GIF • act_Listen.GIF
Subforms	• UCPlayer • (DisplayFwrdContent) • (UCItems) • (UCVoiceNote) • (VoiceDeliveryOptions)
Script libraries	• Core UC Classes • Core UC Strings • Unified Communications

Address Book Server, Message Store Server, and Mail Drop Server

Cisco Unity interacts with Domino servers that perform a variety of functions. Depending on the number of Domino users, these functions may be all on one Domino server or spread out across many servers:

- Address book servers are the servers on which Cisco Unity accesses Domino address books. There are three types of address book:
  - The primary address book (commonly names.nsf) is the address book in which Cisco Unity creates Person documents with mail files for the default accounts and for distribution lists, and from which Domino user data is imported to create Cisco Unity subscribers.

    The primary address book is the home of the Cisco Unity system mailbox; this mailbox sends voice messages from outside callers. (Voice messages from Cisco Unity subscribers are identified as coming from those subscribers.) Each Cisco Unity server must have a system mailbox.

    You choose the primary address book server during Cisco Unity installation.

  - A secondary address book is an address book from which subscribers can be imported but that does not home default Cisco Unity accounts. You can choose a secondary address book, if any, in the Cisco Unity Administrator.
  - Monitored address books may be needed when there are multiple Cisco Unity servers that will be set up for Digital Networking. For more information, see the "Managing Monitored Address Books" section in the "Digital Networking" chapter of the *Networking Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
- Message store servers are the Domino servers that home the mail files for Cisco Unity subscribers. Domino administrators configure mail files for Domino users.
- The mail drop server is the Domino server that the installer specifies while installing IBM Lotus Notes on a Cisco Unity server. Cisco Unity delivers all voice messages to Mail.box on the mail drop server for routing.

Windows Domains and Domino Domains

A Cisco Unity server can be either a domain controller or a member server in a Windows Server 2003 or Windows 2000 Server domain. If the Cisco Unity server is a member server, it should reside in the same highly available and connected network as a domain controller for that domain.

The customer needs at least one Cisco Unity server for each Domino domain that will home Cisco Unity subscribers.

Server Placement

Revised May 6, 2008

Note the following best practices for placement of Cisco Unity servers and the servers that Cisco Unity relies on:

- The Cisco Unity server should reside in the same highly available and connected network as the address book servers, the message store servers, and the mail drop server, or the customer will experience delays in message access, in directory replication, and in directory lookups.
- Ensure that Cisco Unity can resolve server names to IP addresses. If this is not possible on a given network segment, consider adding the necessary resource or moving the Cisco Unity server to a segment that provides easy access to these services.
- Cisco Unity can coexist with firewalls. However, note that Cisco Unity should never be deployed outside of a firewall. Doing so can expose the Cisco Unity server to unwanted intrusion from the Internet, even if the server is hardened.

  When failover or standby redundancy is configured, the Cisco Unity servers cannot be separated from one another by a firewall. They also cannot be separated by a firewall from:

  - Domino servers on which mailboxes for Cisco Unity subscribers are homed.
  - The Domino server that Cisco Unity monitors for changes to the directory.
  - The Domino server to which Cisco Unity sends voice messages. (This is the Domino server that the installer specifies while installing IBM Lotus Notes on the Cisco Unity server. Cisco Unity delivers all voice messages to Mail.box on this server for routing.)
  - The domain controller on which the Cisco Unity installation and services accounts were created.

For additional firewall requirements, see the section "Network Requirements" in the *System Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html:

- A single Cisco Unity server can service both local and remote subscribers, especially when Cisco Unity is integrated with Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager), and when Cisco Unity is configured for Unified Messaging. In a Voice Messaging configuration, the message store server must be in the same location as the Cisco Unity server.
- If Cisco Unity is integrated with a circuit-switched phone system by using voice cards, ensure that the Cisco Unity server is within the maximum allowable cable length of the phone system. If Cisco Unity is integrated with Cisco Unified CM or via PIMG or TIMG units, the distance between the servers is less crucial.

Active Directory Accounts and Permissions

Cisco Unity requires that three Active Directory domain accounts be created during installation, as described in the Cisco Unity installation guide. One account is used to install Cisco Unity, another is the account that most Cisco Unity services log on as, and the third is used to access the Cisco Unity Administrator. (Some services, including the Text to Speech service and the service that controls Cisco Unity licensing, log on as the local system account.)

The permissions required by each of the accounts are set by the Cisco Unity Permissions Wizard. The account that Cisco Unity services log on as can be used by more than one Cisco Unity server in the same domain. For detailed information on the permissions required, see the Help file *Permissions Granted by the Cisco Unity 5.0(1)+ Permissions Wizard* at http://ciscounitytools.com/HelpFiles/PW501/PWHelpPermissionsSet_ENU.htm.

These accounts and permissions are required for Cisco Unity–specific functionality and are separate from the Domino permissions that are described in the "Domino Permissions" section on page 5-7.

Domino users who are Cisco Unity subscribers do not need Active Directory accounts, and Cisco Unity administrators and subscribers are not required to use Windows authentication.

Authentication

Cisco Unity subscribers whose class of service (COS) allows them access to the Cisco Unity Administrator can log on to the Cisco Unity Administrator by using Domino authentication, Integrated Windows authentication, or Anonymous authentication, depending on how the system is configured. Subscribers whose COS allows them access to the Cisco Unity Assistant must log on to the Cisco Unity Assistant by using Domino authentication.

For more information, see:

- The "Managing Cisco Unity Administrator Accounts" chapter in the *System Administration Guide for Cisco Unity Release 5.x (With IBM Lotus Domino)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.
- The "Accessing and Using the Cisco Unity Administrator" chapter, also in the *System Administration Guide for Cisco Unity Release 5.x (With IBM Lotus Domino)*.
- The "Authentication for Cisco Unity Applications" chapter in the *Security Guide for Cisco Unity Release 5.x (With IBM Lotus Domino)*, also at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Domino Permissions

Before Cisco Unity is installed, the Cisco Unity installer or a qualified Domino administrator needs to:

- Create a group for Cisco Unity servers named UnityServers, and grant the group Editor permissions for Admin4.nsf and Editor with Delete Documents permissions for Names.nsf.
- Confirm that the UnityServers group has the permissions required to create databases and templates. This allows Cisco Unity to create mail files for the default accounts.

With these permissions, Cisco Unity acts as a Notes user to:

- Import data from the Domino address book to create Cisco Unity subscribers, contacts, and distribution lists.
- Change the Domino address book by using the Cisco Unity Administrator.
- Submit voice messages through Domino.
- Retrieve and play messages left for subscribers.
- Get information about the read/unread status of voice messages, e-mail, and fax messages in a subscriber mailbox, and send notification when there are new messages.

In addition, when a Domino user is imported into Cisco Unity, Cisco Unity submits an AdminP request to grant the user access to the imported user mail file.

For more information on setting Domino-specific permissions, see the applicable Cisco Unity installation guide, at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Cisco Unity Subscribers and Domino Users

A Cisco Unity subscriber is a Domino user who has been DUC for Cisco-enabled and imported into Cisco Unity. The person document of each subscriber has Cisco Unity attributes, and the mail file has DUC for Cisco attributes. The only way to create a Cisco Unity subscriber is to import an existing Domino user into Cisco Unity. Cisco Unity cannot create Domino users by using the Cisco Unity Administrator.

Domino Clusters

Cisco Unity supports homing Cisco Unity subscribers on Domino clusters. The Domino cluster must meet all IBM Lotus requirements, particularly those related to the maximum number of users and to supported hardware.

Depending on the number of users on a cluster, the customer may want to install one Cisco Unity server for each Domino cluster.

The customer is responsible for installing, configuring, and maintaining the Domino cluster.

For more information on Domino clusters, refer to the Lotus Domino documentation, available on the Lotus Domino website.

Message Routing

Cisco Unity voice messages are routed to Domino mailboxes by Domino. When a caller leaves a voice message (whether an outside caller or a subscriber), Cisco Unity submits the messages to Mail.box on the mail drop server. The mail drop server determines the routing path to the mail file of the recipient. When Cisco Unity has given the message to the mail drop server, the Domino services are responsible for delivery.

Notes Client on the Cisco Unity Server

For Cisco Unity to interact with a Domino server, a Notes Client must be installed on the Cisco Unity server. No other Domino software is installed on the Cisco Unity server. In order to determine the correct version of the Notes client to use, see the "Domino Requirements—Message Store" section of *System Requirements for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Client Access Licenses

DUC for Cisco is automatically shipped by Cisco with all Cisco Unity for Domino systems.

The customer is responsible for purchasing and maintaining any other Lotus licenses that may be required.

Backing Up and Restoring Data

Backing up mailboxes is important in any Unified Messaging deployment. The customer should use a backup program qualified by IBM Lotus for use with Domino.

Migrating from Cisco Unity for Exchange

Cisco Unity for Exchange systems, configured either for Voice Messaging or Unified Messaging, can be converted to Cisco Unity 5.0 for Domino, but only by reinstalling all software, and losing Cisco Unity settings and voice messages.

Cisco Unity and the Domino Address Book

Cisco Unity for Domino uses a Domino address book as its directory service. However, the majority of information on Cisco Unity subscribers and other Cisco Unity objects appears only in a SQL Server/MSDE database. For the small amount of data that appears both in the Domino address book and in the Cisco Unity database (for example, extension), Cisco Unity periodically checks the Domino address book for changes and replicates those changes in the Cisco Unity database. Some of the changes that are made in the Cisco Unity Administrator are replicated to the Domino address book. After a Cisco Unity system is installed and running, changes to the address book and to settings in the Cisco Unity Administrator are relatively few in number, so this replication will not hurt performance.

Cisco Unity requires Editor with Delete Documents permission for the address book that Cisco Unity monitors. A Cisco Unity server can monitor the address books for one domain, including Names.nsf and any secondary address book that may be supporting proxy/remote users (users who do not have mail files in the Domino domain).

For more information on permission requirements, see the applicable Cisco Unity installation guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Unified Messaging Configurations

In a Unified Messaging configuration, Cisco Unity does not own the directory or messaging data but instead uses existing directory (Domino address book) and message store information. The benefits of Unified Messaging include:

- Significantly reduced administrative overhead because the customer does not need to create and maintain separate accounts for e-mail and voice messaging applications.
- No dedicated infrastructure for a separate voice-messaging system. Cisco Unity uses the existing messaging infrastructure by voice-enabling the e-mail environment.
- Starting with Unified Messaging is administratively easier than starting with a Voice Messaging system and later migrating to Unified Messaging.

Unified Messaging, No Domino Cluster

When you are setting up two or more Cisco Unity servers, the servers can be networked by using Cisco Unity Digital Networking. If the phone system has ports available, you can hook up more than one Cisco Unity server to each phone system. For more information, see Table 5-3.

Table 5-3 Server Requirements and Recommendations for a Unified Messaging Configuration

Servers	Requirements and Recommendations
Cisco Unity server	Each physical site that includes one or more Domino servers on which mailboxes for Cisco Unity subscribers are homed also includes at least one Cisco Unity server. Each Domino domain requires a Cisco Unity server. If you need to import Cisco Unity subscribers in different Domino domains, you must install a Cisco Unity server in each Domino domain and use Digital Networking between the servers.
Domino address book server, message store server, and mail drop server	Domino servers must be in the same highly available and connected LAN as the Cisco Unity server.
Domain controller/global catalog server (DC/GC)	There must be at least one DC/GC per physical site that includes a Cisco Unity server. If necessary, the Cisco Unity server can be the DC/GC.
DNS server	There must be at least one DNS server per physical site that includes a Cisco Unity server. In sites with enough servers, we recommend two or more DNS servers.
Media gateways (for phone system integrations that include PIMG or TIMG units	The PIMG or TIMG units can be connected to the Cisco Unity server by a LAN or a WAN.
Cisco Unified Communications Manager servers	The Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) and Cisco Unity servers can be connected by a LAN or a WAN.

Table 5-3 Server Requirements and Recommendations for a Unified Messaging Configuration (continued)

Servers	Requirements and Recommendations
Cisco Unified Communications Manager Express	The Cisco Unified Communications Manager (CM) Express (formerly known as Cisco Unified CallManager Express) and Cisco Unity servers must be connected by a LAN.
Cisco Unity voice-recognition server	The Cisco Unity voice-recognition server and the Cisco Unity server must be connected by a LAN. For each Cisco Unity server that homes subscribers for whom you want to have voice-recognition functionality, you must have one voice-recognition server. A voice-recognition server cannot service more than one Cisco Unity server or, when failover is configured, one pair of failover servers. Voice-recognition software cannot be installed on the Cisco Unity server.
Cisco Unity Bridge server	The Bridge server can be a member server in an existing domain or a workgroup server. It cannot be a DC/GC. The Cisco Unity Bridge and Cisco Unity servers can be connected by a LAN or a WAN. Bridge software cannot be installed on the Cisco Unity server. For more information, see the *Design Guide for Cisco Unity Bridge* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_implementation_design_guides_list.html.

Unified Messaging, Domino Cluster

A clustered environment is the same as the non-clustered environment detailed in Table 5-3 except that all Domino servers have to be in the same highly available and connected LAN as the Cisco Unity server.

Domino partitioning is also supported.

Voice Messaging Configuration

A clustered environment is the same as the environment detailed in Table 5-3 except that all Domino servers are dedicated to servicing Cisco Unity voice messages.

Criteria for a Supported Configuration

Requirements for supported configurations for Cisco Unity for Domino include the following:

- Domino servers and Domino clusters must meet all IBM Lotus requirements, including requirements related to DUC for Cisco, the maximum number of users per server, the proper amount of memory, the proper processors and processor speed, hard disks that can meet disk-access response times, and placement of data files and transaction log files. Cisco Unity cannot support message store servers that have performance bottlenecks such as slow hard drives or insufficient memory.
- A Cisco Unity server can service a single physical site, meaning one or more well-connected LANs, such as a campus, single building, or other centralized facility where network bandwidth is not a problem.

- A Cisco Unity server can service mailboxes on up to a recommended maximum of ten Domino servers or clusters in a single physical site.
- A Cisco Unity server can service a single Domino address book (directory or Names.nsf file) for local Cisco Unity data (data for subscribers homed on the local Cisco Unity server) and global Cisco Unity data (data for subscribers homed on other Cisco Unity servers).
- A Cisco Unity server can service a single secondary address book for contacts. The secondary address book must have the same views as Names.nsf, and must be DUC for Cisco-enabled (must contain the DUC for Cisco admin view). The secondary address book can reside on a different Domino server in the same Domino domain.
- Two or more Cisco Unity servers can be installed in a single Domino domain. Subscribers who are homed on one Cisco Unity server can send voice messages to subscribers who are homed on another Cisco Unity server by using Cisco Unity Digital Networking.
- Cisco Unity for Domino subscribers and Cisco Unity for Exchange subscribers can send voice messages to one another by using VPIM Networking.
- Cisco Unity for Domino subscribers in one Domino domain can send voice messages to subscribers in another Domino domain by configuring monitored address books as described in the "Managing Monitored Address Books" section in the "Digital Networking" chapter of the *Networking Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Deploying Cisco Unity for Lotus Domino

Cisco Unity for Lotus Domino can be deployed in the following ways:

- Unified Messaging with one or more Cisco Unity servers servicing Cisco Unity subscribers on multiple Domino servers in the same Domino domain and the same well-connected network.
- Unified Messaging with access to Cisco Unity Assistant and DUC for Cisco (the form in Notes that allows subscribers to play and record messages).
- Unified Messaging with multiple Cisco Unity servers. This requires either Cisco Unity Digital Networking (if two or more Cisco Unity servers are in the same Domino domain) or SMTP gateways and Internet subscribers (if two or more Cisco Unity servers are in separate Domino domains). For more information, see the *Networking Guide for Cisco Unity*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
- Voice Messaging.

See the following sections for additional information:

- Administrative Access and Control, page 5-12
- Establishing Support Policies, page 5-12
- Network Services, page 5-12
- Deployment Tasks for Unified Messaging Configurations, page 5-12
- Operational Tasks, page 5-13

Administrative Access and Control

To manage administrative access to the Cisco Unity server and its resources, the customer may want different levels of access for different operations, for example, backing up the server or gathering performance information for trending.

When installing Cisco Unity in a Unified Messaging configuration, it is best to allow administrative access to the server to be governed by the server administration policies of the customer. This should not detract from the administrative access required for normal Cisco Unity operations, which include:

- Managing the server resources (hardware, operating system, file system, and other supporting software).
- Managing the Cisco Unity application, including web access; supporting components such as SQL Server/MSDE, IIS, and Internet Explorer; the Cisco Unity application log files; and utilities such as the Windows Event Viewer, Performance Monitor, and so on.
- Administering Cisco Unity subscribers, distribution lists, call handlers, and so on.
- Administering Cisco Unity switch connectivity to Cisco Unified Communications Manager or a circuit-switched phone system.

Establishing Support Policies

To make administering Cisco Unity more manageable, establish a support policy that separates Cisco Unity-specific administration from administration for the rest of the server. This allows Cisco Unity administrators with limited class of service (COS) settings to access the Cisco Unity application only as designed through their COS.

Network Services

Cisco Unity is a Notes client that uses Notes name resolution to resolve FQDNs in the Domino/Notes environment. Cisco Unity must be able to access and resolve server names across the deployment, or performance will suffer and some Cisco Unity operations will fail. Ideally, the name resolution server will be on the same highly available network as the Cisco Unity server. Because Cisco Unity for Domino can only be deployed in existing Domino environments, name resolution servers should already be available.

Because Cisco Unity still needs to be installed in an Active Directory domain, Cisco Unity relies on Windows DNS. If you install Cisco Unity into an existing Active Directory domain, there should be an existing DNS server highly available. If the customer does not have an existing Active Directory domain, DNS must be installed on the Cisco Unity server.

Deployment Tasks for Unified Messaging Configurations

In a Unified Messaging configuration, pay careful attention to the placement of Cisco Unity servers, how they are managed, and the accounts that are used to manage them.

Consider the following deployment best practices:

- Define and create the accounts to be used in running the Cisco Unity services.
- Define and create the accounts to be used to administer Cisco Unity.

- Create a group for Cisco Unity servers, and grant the group Editor permissions for Admin4.nsf, and Editor with Delete Documents permissions for Names.nsf.
- Install DUC for Cisco components on the applicable Domino servers.
- Define the level of access to the local Cisco Unity server necessary for an administrator. Subscribers who are not administrators do not need direct access to the Cisco Unity server operating system or file system.
- Define a policy for Cisco Unity classes of service for each Cisco Unity server.
- Define the Cisco Unity templates to be used for subscribers.
- Define the Cisco Unity distribution lists for each installation. (Other than the default distribution lists created during installation, you must either identify existing distribution lists in the Domino address book or create new distribution lists, and then import them into Cisco Unity.)
- Define any audio-text applications that need to be created on each Cisco Unity server.
- Define dialing restrictions necessary to prevent subscribers from accessing unauthorized outside numbers.
- Verify that the number of subscribers serviced by each Cisco Unity server is known and documented (there is a limit of 7,500 subscribers per Cisco Unity server).
- Verify that each Cisco Unity server is properly sized for the number of subscribers it will service. For additional sizing information, see the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.
- Create and document a suitable disaster recovery plan.
- Verify that the switch integration is understood.
- Determine the number of ports needed for message notification, and for recording and playing messages over the phone.
- Verify that all hardware and supporting components are set up correctly.
- List the acceptance tests to be run after the server is installed and before going live.
- Verify that there is a fallback procedure in the event that problems are encountered.
- Define any measurements necessary to benchmark the initial performance of the system.
- Install the DUC for Cisco client on workstations for Cisco Unity subscribers. This is necessary before a Domino user can be imported into Cisco Unity as a subscriber.

Operational Tasks

The following are best practices for an operational Cisco Unity system:

- Create and implement a regular maintenance schedule to gather logs and to monitor the use of server resources such as disk space, memory, and the CPU.
- Verify that regular backups are occurring.
- Make arrangements for any regular downtime necessary for offline maintenance activities.
- Make arrangements for any special administrative tasks, for example maintaining and creating audio-text applications and running clean up utilities such as Directory Walker.
- Before reconfiguring the system, for example when migrating from Voice Messaging to Unified Messaging or when upgrading hardware, mock up the existing Cisco Unity system in a lab environment, and test and validate the work.

Feature Parity Between Cisco Unity for Domino and Cisco Unity for Exchange

Cisco Unity 5.0 for Domino does not support:

- Cisco Unity reports.
- The Cisco Unity Inbox.
- Using an IMAP e-mail client to access Cisco Unity voice messages.
- The secure messaging feature.

The following capabilities of Cisco Unity for Exchange are not available in Cisco Unity for Domino:

- Creating a Cisco Unity subscriber and the corresponding Domino user by using the Cisco Unity Administrator. In Cisco Unity for Domino, a subscriber must first be created as a Domino user and then imported into Cisco Unity.
- Functionality of the Deleted Items folder.
- Future delivery.
- Mailbox status.
- Mailbox size.
- Sending broadcast messages to subscribers who are homed on more than one Cisco Unity server.
- Automatic VPIM subscriber directory updates.

The following Cisco Unity tools are not available with Cisco Unity for Domino:

- Extension Address Utility.
- FullDB Import.
- FullDB Export.
- Message Store Manager.
- Move Subscriber Data.
- Public DL Builder.

CHAPTER 6

Integrating Cisco Unity with the Phone System

See the following sections:

- Overview, page 6-1
- How an Integration Works, page 6-2
- Sample Path for a Call from the Phone System to a Subscriber, page 6-8
- General Integration Issues, page 6-9
- Integrating with Cisco Unified Communications Manager (by Using SCCP or SIP), page 6-10
- Integrating with Cisco Unified Communications Manager Express (by Using SCCP or SIP), page 6-17
- Integrating by Using SIP, page 6-22
- Integrating with Circuit-Switched Phone Systems by Using PIMG or TIMG Units, page 6-24
- Integrating with Multiple Phone Systems, page 6-30
- Optional Integration Features, page 6-32
- Centralized Voice Messaging, page 6-34

Overview

An integration enables communication between Cisco Unity and a phone system, providing subscribers with features that typically include the following:

- Calls to a subscriber extension that does not answer or is busy are forwarded to the subscriber personal greeting.
- Messages left for a subscriber activate the message waiting indicator (MWI) on the extension.
- A subscriber has easy access to messages by pressing a button on the phone and entering a password.

Depending on the phone system and the integration, other integration features may be available, including caller ID, call forward to the subscriber busy greeting, and identified subscriber messaging.

For a list of supported phone systems, see *Supported Hardware and Software, and Support Policies for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Cisco Unity can integrate with one or more phone systems at the same time. For details, see the *Multiple Phone System Integration Guide for Cisco Unity 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Circuit-switched phone systems can integrate with Cisco Unity by using one of the following integration methods:

PIMG/TIMG integrations	PIMG or TIMG units are media gateways between circuit-switched phone systems and IP networks. On the circuit-switched phone system side, there are digital (feature-set), analog, and T1-CAS interfaces. On the IP side, there is a SIP interface, which is how Cisco Unity communicates with the PIMG unit. PIMG/TIMG units are the preferred method for integrating with circuit-switched phone systems.
Voice card integrations	Voice cards connect circuit-switched phone systems and Cisco Unity through analog lines. Voice cards must be installed in the Cisco Unity server or in an expansion chassis that is connected to the Cisco Unity server. Support for voice cards is slowly being phased out, and voice cards are now only supported when Windows 2000 Server is installed on the Cisco Unity server. For information on the voice cards supported for use with Cisco Unity, see *Supported Hardware and Software, and Support Policies for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

For detailed information on integrating Cisco Unity with a specific phone system, see the applicable Cisco Unity integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

How an Integration Works

An integration depends on the following components to be successful:

- Lines and cables necessary to make physical connections (in circuit-switched phone systems) or a network connection (in Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) and SIP proxy servers). For more information, see the "Lines and Cables to Make Physical Connections" section on page 6-3.
- Settings in the phone system and in Cisco Unity. For more information, see the "Settings in the Phone System and in Cisco Unity" section on page 6-7.
- Call information exchanged by the phone system and Cisco Unity. For more information, see the "Call Information Exchanged by the Phone System and Cisco Unity" section on page 6-7.
- Call control (signals used to set up, monitor, and tear down a call) to determine and control the status of the call. For more information, see the "Call Control" section on page 6-8.

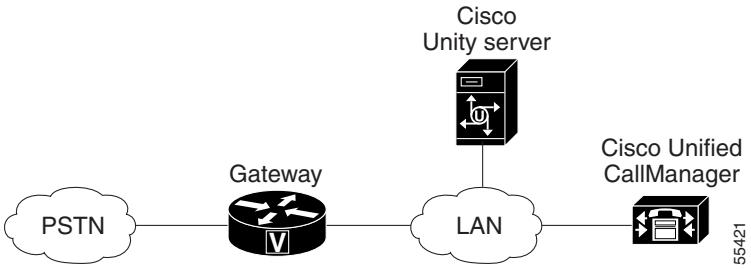
Lines and Cables to Make Physical Connections

Depending on the type of integration, different combinations of lines and cables are used to connect the phone system and Cisco Unity.

Integration with Cisco Unified Communications Manager

Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) and SIP proxy servers use network connections that carry all communication to and from Cisco Unity. Figure 6-1 shows the network connections used in an integration with Cisco Unified CM.

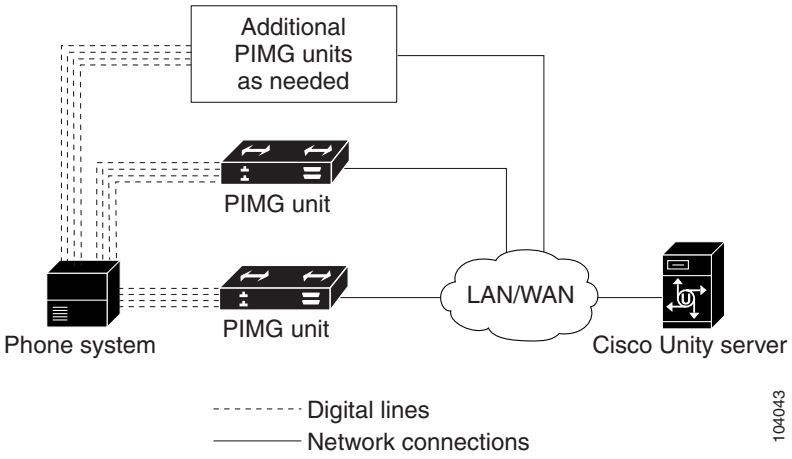
Figure 6-1 Connections for an Integration with Cisco Unified Communications Manager



Digital Integration with Digital PIMG Units

The phone system sends call information, MWI requests, and voice connections through the digital lines, which connect the phone system to the PIMG units. The PIMG units communicate with the Cisco Unity server through the LAN or WAN by using Session Initiation Protocol (SIP). Figure 6-2 shows the connections used in a digital integration by using digital PIMG units.

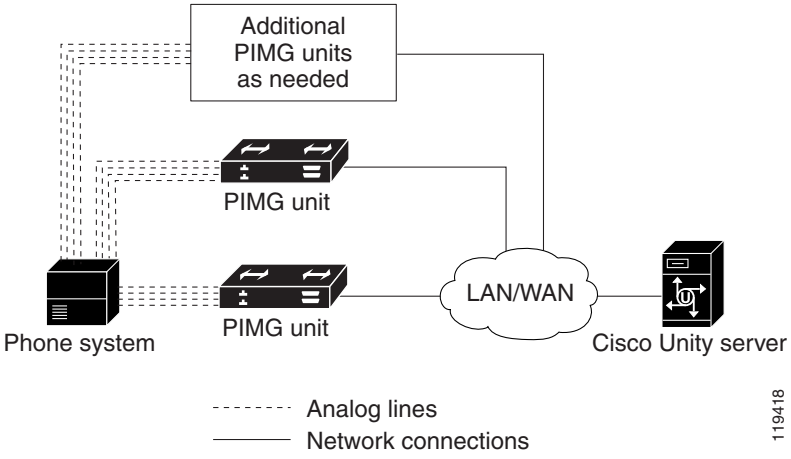
Figure 6-2 Connections for a Digital Integration by Using Digital PIMG Units



DTMF Integration with Analog PIMG Units

The phone system sends call information, MWI requests, and voice connections through the analog lines, which connect the phone system to the PIMG units. The PIMG units communicate with the Cisco Unity server through the LAN or WAN by using Session Initiation Protocol (SIP). Figure 6-3 shows the connections for a DTMF integration by using analog PIMG units.

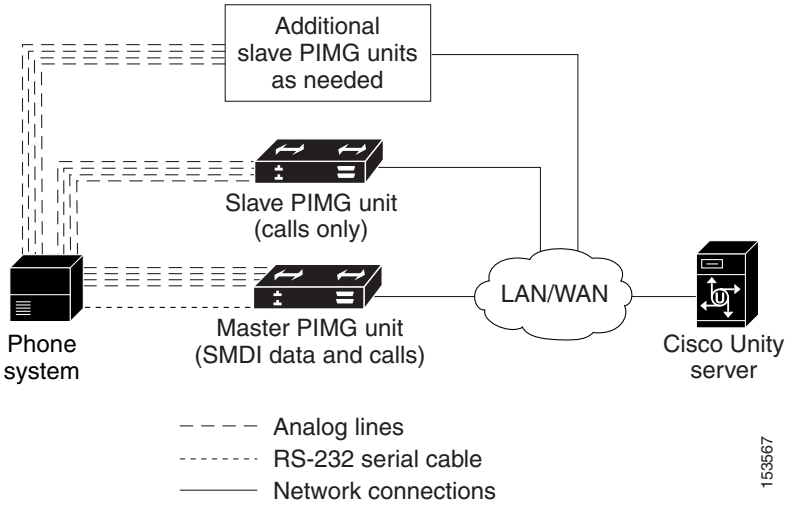
Figure 6-3 Connections for a DTMF Integration by Using Analog PIMG Units



Serial (SMDI, MCI, or MD-110) Integration with Analog PIMG Units

The phone system sends call information and MWI requests through the data link, which is an RS-232 serial cable that connects the phone system and the master PIMG unit. Voice connections are sent through the analog lines between the phone system and the PIMG units. The PIMG units communicate with the Cisco Unity server through the LAN or WAN by using Session Initialization Protocol (SIP). Figure 6-4 shows the connections for a serial integration by using analog PIMG units.

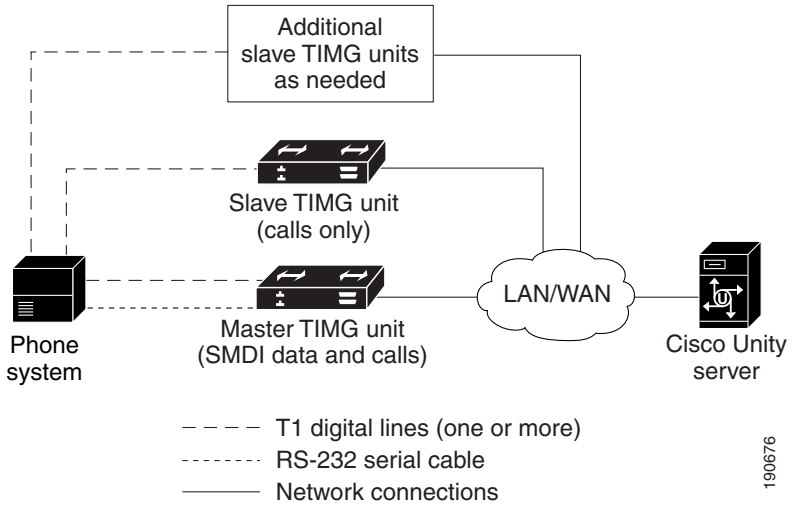
Figure 6-4 Connections for a Serial (SMDI, MCI, or MD-110) Integration by Using Analog PIMG Units



TIMG Integration

The phone system sends call information and MWI requests through the data link, which is an RS-232 serial cable that connects the phone system and the master TIMG unit. Voice connections are sent through the T1 digital lines between the phone system and the TIMG units. The TIMG units communicate with the Cisco Unity server through the LAN or WAN by using Session Initialization Protocol (SIP). Figure 6-5 shows the connections.

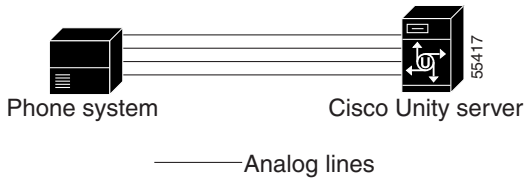
Figure 6-5 Connections for an Integration by Using TIMG Units



DTMF Integration with Voice Cards

The circuit-switched phone systems use analog lines to carry voice connections, call information, and MWI activation requests. The lines connect the ports on the phone system to the voice messaging ports on voice cards installed on the Cisco Unity server. Signaling carried across the analog lines is achieved through DTMF digits being sent to and from the phone system and Cisco Unity. For example, in order for Cisco Unity to turn on or off the MWI lamp, DTMF digits (including #, *, and the digits 0–9) are sent from Cisco Unity to the phone system. Figure 6-6 shows the connections used in a DTMF integration.

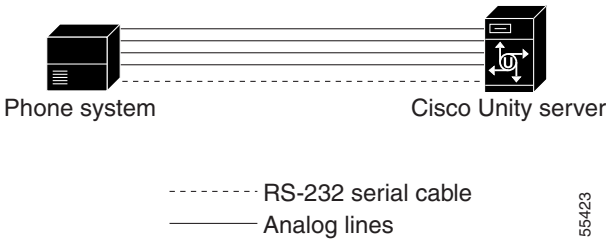
Figure 6-6 Connections for a DTMF Integration by Using Voice Cards



Serial Integration with Voice Cards

In serial integrations (also called SMDI or MCI integrations for NEC phone systems), circuit-switched phone systems use an RS-232 serial cable to carry call information and MWI activation requests. The serial cable connects the serial port on the phone system to the serial port on the Cisco Unity server. (Some phone systems require hardware such as a modem or PBXLink box to connect to the serial cable.) Figure 6-7 shows the connections.

Figure 6-7 Connections for a Serial Integration by Using Voice Cards



Settings in the Phone System and in Cisco Unity

For an integration to be successful, Cisco Unity and the phone system must know the connections to use (for example, cables, IP addresses, and channels) and the expected method of communication (for example, IP packets, serial packets, or DTMF tones). Certain integrations require specific codes or extensions for turning MWIs on and off.

There are required settings for Cisco Unity, and programming for the phone system, that must be made in order to enable the integration. For information on these settings, see the applicable integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Call Information Exchanged by the Phone System and Cisco Unity

The phone system and Cisco Unity exchange call information to manage calls and to make the integration features possible. With each call, the following call information is typically passed between the phone system and Cisco Unity:

- The extension of the called party.
- The extension of the calling party (for internal calls) or the phone number of the calling party (if it is an external call and the phone system supports caller ID).
- The reason for the forward (the extension is busy, does not answer, or is set to forward all calls). There is also a reason code for Direct Calls.

Cisco Unified Communications Manager SCCP and SIP trunk integrations can also provide the following call information (the choice of first and last redirecting number is set in the Advanced Settings Tool, which is available in Tools Depot):

- Called number
- First redirecting number
- Last redirecting number

Note Cisco Unity can use either the first redirecting number or last redirecting number, depending on the setting in the Advanced Settings Tool, which is available in Tools Depot.

If the phone system sends the necessary information and if Cisco Unity is configured correctly, an integration can provide the following integration functionality:

- Call forward to personal greeting
- Call forward to busy greeting
- Caller ID
- Easy message access (a subscriber can retrieve messages without entering an ID because Cisco Unity identifies the subscriber based on the extension from which the call originated; a password may be required)
- Identified subscriber messaging (Cisco Unity identifies the subscriber who leaves a message during a forwarded internal call, based on the extension from which the call originated)
- Message waiting indication (MWI)

Call Control

The phone system uses a set of signals to set up, monitor, and release connections for a call. Cisco Unity monitors call control signals to determine the state of the call, and uses these signals to respond appropriately to phone system actions and to communicate with the phone system. For example, a caller who is recording a message might hang up, so Cisco Unity detects that the call has ended and stops recording.

Depending on the phone system, the following types of call control signals are used:

Cisco Unified Communications Manager	For Skinny Call Control Protocol (SCCP) integrations, Cisco Unified Communications Manager generates SCCP messages, which are translated by the Cisco Unity-CM TSP into TAPI that Cisco Unity uses. Cisco Unity actions—such as hook flash for transferring calls—are translated by the Cisco Unity-CM TSP into the SCCP messages that Cisco Unified CM uses. For SIP trunk integrations, Cisco Unified CM sends SIP messages, and Cisco Unity sends SIP responses when a call is set up or terminated.
Circuit-switched phone system	For PIMG/TIMG integrations, the phone system sends messages to the PIMG or TIMG units, which send the applicable SIP messages to Cisco Unity. Cisco Unity sends SIP responses when a call is set up or terminated, and the PIMG or TIMG units communicate with the phone system. For voice card integrations, the phone system generates and responds to in-band signaling (for example, busy, disconnect, DTMF, and hook flash). The signaling tones are translated by the Dialogic TSP into TAPI events that Cisco Unity can use. Cisco Unity makes a telephony request such as “transfer,” which is translated by the Dialogic TSP into the signal (hook flash) that the phone system can use.

Sample Path for a Call from the Phone System to a Subscriber

The following steps give an overview of a sample path that an external call can take when traveling from the phone system to a subscriber.

1. For Cisco Unified Communications Manager, when an external call arrives, the gateway sends the call over the LAN or WAN to Cisco Unified CM.

The corresponding step for circuit-switched phone systems, when an external call arrives via the PSTN, TI/PRI, DID or LS/GS analog trunks, is for the call to be routed through the phone system to the Cisco Unity voice mail pilot number.

2. The phone system routes the call to an available Cisco Unity extension (a voice messaging port).
3. Cisco Unity answers the call and plays the opening greeting.
4. During the opening greeting, the caller enters an extension. For example, the caller enters 1234 to reach a person with that extension.
5. Cisco Unity notifies the phone system that there is a call for extension 1234.
6. Depending on whether Cisco Unity is set up to perform a supervised transfer or a release transfer, the following occurs:

Supervised transfer	While Cisco Unity holds the call, the phone system attempts to establish a connection with extension 1234. If the line is available, the phone system connects the call from Cisco Unity to extension 1234. The phone system and Cisco Unity drop out of the loop, and the call is connected directly from the original caller to extension 1234. If the line is busy or unanswered, the phone system gives that information to Cisco Unity, and Cisco Unity performs the operation the subscriber has specified. For example, Cisco Unity takes a message.
Release transfer (blind transfer)	Cisco Unity passes the call to the phone system, and the phone system sends the call to extension 1234 without waiting to determine whether the line is available. Then the phone system and Cisco Unity drop out of the loop. In this configuration, if the customer wants Cisco Unity to take a message when a line is busy or unanswered, each phone must be configured to forward calls to Cisco Unity when the line is busy or unanswered.

General Integration Issues

For a detailed list of the requirements for a specific integration, see the applicable Cisco Unity integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

If Cisco Unity is configured for failover, line connections between the phone system and the Cisco Unity servers are described in the following documents:

- The applicable Cisco Unity integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.
- The *Failover Configuration and Administration Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

In addition, consider the following list of integration issues:

- Cisco Unified Communications Manager integrates with Cisco Unity only through a network connection.
- Circuit-switched phone systems that connect to PIMG or TIMG units integrate with Cisco Unity only through a network.

- Circuit-switched phone systems that connect to voice cards and that use an RS-232 serial cable for the integration must be within 50 feet of the Cisco Unity server. For serial cable specifications, see the applicable Cisco Unity integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.
- Voice card integrations are supported only when Windows 2000 Server is installed on the Cisco Unity server. For a list of supported voice cards, see *Supported Hardware and Software, and Support Policies for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
- The license file for Cisco Unity may enable more voice messaging ports than the customer needs. Install only the number of ports that are needed, so that system resources are not allocated to unused ports, and do not exceed the port limitations set for the platform. For more information, see the *Cisco Unity Supported Platform List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html). For additional information about configuring voice messaging ports, see the "Planning How the Voice Messaging Ports Will Be Used in Cisco Unity" section in the applicable Cisco Unity integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Integrating with Cisco Unified Communications Manager (by Using SCCP or SIP)

Cisco Unity supports Cisco Unified Communications Manager (CM) (formerly known as Cisco Unified CallManager) integrations through both SCCP and SIP interfaces. Table 6-1 shows the major differences in these integration methods.

Table 6-1 Differences Between SCCP and SIP Integration Methods

Feature	SCCP	SIP
Communication method	Cisco Unity-CM TSP	SIP trunk
Failover	Supported	Not supported
Use of SCCP and SIP phones	Supported	Some SCCP phones may require use of a media termination point (MTP)
Support for Cisco Unified CM versions	All versions	Versions 5.x and later
Cisco Unified CM versions 5.x and later	Supported	Supported
Cisco Unified CM authentication and encryption	Supported	Not supported
First/last redirecting number	Supported	Supported
QOS	Supported	Supported

For information on the compatibility of Cisco Unity and Cisco Unified CM versions with the Cisco Unity-CM TSP and the SIP trunk, see the following documents at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html:

- *SCCP Compatibility Matrix: Cisco Unity, the Cisco Unity-CM TSP, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express*
- *SIP Trunk Compatibility Matrix: Cisco Unity and Cisco Unified Communications Manager*

For information on how to integrate Cisco Unity with Cisco Unified CM, see the applicable Cisco Unity integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

For more information on using the SIP protocol to integrate Cisco Unity with Cisco Unified CM, see the "Integrating by Using SIP" section on page 6-22.

Note When the G.729a codec is used, Cisco Unity cannot perform silence detection. Using this codec may result in messages that have long trailing silence or that are entirely silent.

Integrating Cisco Unity with Multiple Versions of Cisco Unified Communications Manager

A single Cisco Unity server can support multiple versions of Cisco Unified CM. The version of the Cisco Unity-CM TSP or SIP trunk being used must support all versions of Cisco Unified CM integrated with Cisco Unity. See the following documents at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html:

- *SCCP Compatibility Matrix: Cisco Unity, the Cisco Unity-CM TSP, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express*
- *SIP Trunk Compatibility Matrix: Cisco Unity and Cisco Unified Communications Manager*

Integrating Cisco Unity with Multiple Cisco Unified Communications Manager Clusters

To integrate Cisco Unity with more than one Cisco Unified CM cluster, you can just re-run the Cisco Unity Telephony Integration Manager, or UTIM. Note the options and considerations detailed in Table 6-2.

Table 6-2 Options and Considerations for Integrating with Multiple Cisco Unified Communications Manager Clusters

Option	Considerations
Create a new Cisco Unified CM integration for each new Cisco Unified CM cluster	• This is the recommended method. • Each Cisco Unified CM integration handles the MWIs for the cluster. Dedicated MWI ports for each Cisco Unified CM cluster is necessary only if the Cisco Unified CM integration has multiple clusters in UTIM. • Cisco Unity sends each MWI request directly to the Cisco Unified CM cluster on which the subscribers is homed. • Multiple Cisco Unified CM integrations can be used with multiple UTIM clusters on a Cisco Unity server.
Add a cluster in UTIM to an existing Cisco Unified CM integration for each new Cisco Unified CM cluster	• You must assign at least one MWI port dedicated to each Cisco Unified CM cluster that you add. • The first cluster in UTIM will handle all calls and direct them to the Cisco Unified CM cluster on which the subscriber is homed. • You can create an unlimited number of clusters in UTIM to a Cisco Unified CM integration. • Multiple UTIM clusters can be used with multiple Cisco Unified CM integrations on the Cisco Unity server.

Within a cluster, it is important to identify the backup (secondary) Cisco Unified CM servers so that Cisco Unity can connect to it if the primary Cisco Unified CM server becomes unavailable.

Cisco Unified Communications Manager Authentication and Encryption for Cisco Unity Voice Messaging Ports (SCCP Integrations Only)

A potential point of vulnerability for a Cisco Unity system is the connection between Cisco Unity and Cisco Unified Communications Manager. Possible threats include:

- Man-in-the-middle attacks, in which an attacker intercepts and changes the data flowing between Cisco Unified CM and Cisco Unity voice messaging ports.
- Network traffic sniffing, in which an attacker captures phone conversations and signaling information that flow between Cisco Unified CM, the Cisco Unity voice messaging ports, and IP phones that are managed by Cisco Unified CM).
- Changing the call signaling between the Cisco Unity voice messaging ports and Cisco Unified CM.
- Changing the media stream between Cisco Unity voice messaging ports and endpoints, for example, phones or gateways.

- Identity theft of the Cisco Unity voice messaging port, in which a non-Cisco Unity device presents itself to Cisco Unified CM as a Cisco Unity voice messaging port.
- Identity theft of the Cisco Unified CM server, in which a non-Cisco Unified CM server presents itself to Cisco Unity voice messaging ports as a Cisco Unified CM server.

Note SIP integrations do not support Cisco Unified CM authentication or encryption.

See the following sections for additional details:

- Cisco Unified Communications Manager Security Features, page 6-13
- When Data Is Encrypted, page 6-15
- Cisco Unified Communications Manager Cluster Security Mode Settings in Cisco Unity, page 6-15
- Disabling and Re-Enabling Security, page 6-16
- Multiple Integrations Can Have Different Security Mode Settings, page 6-16
- Settings for Individual Voice Messaging Ports, page 6-16

Cisco Unified Communications Manager Security Features

Cisco Unified CM 4.1(3) or later can secure the connection with Cisco Unity against these threats. The Cisco Unified CM security features that Cisco Unity can take advantage of are described in Table 6-3.

Table 6-3 Cisco Unified Communications Manager Security Features That Are Used by Cisco Unity

Security Feature	Description
Signaling authentication	Uses the Transport Layer Security (TLS) protocol to validate that no tampering has occurred to signaling packets during transmission. Signaling authentication relies on the creation of the Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and the Cisco Unity voice messaging ports. • Modification of the call signaling. • Identity theft of the Cisco Unity voice messaging port. • Identity theft of the Cisco Unified CM server.
Device authentication	Validates the identity of the device. This process occurs between Cisco Unified CM and Cisco Unity voice messaging ports when each device accepts the certificate of the other device. When the certificates are accepted, a secure connection between the devices is established. Device authentication relies on the creation of the Cisco Certificate Trust List (CTL) file. This feature protects against: • Man-in-the-middle attacks that modify the information flow between Cisco Unified CM and the Cisco Unity voice messaging ports. • Modification of the media stream. • Identity theft of the Cisco Unity voice messaging port. • Identity theft of the Cisco Unified CM server.

Table 6-3 Cisco Unified Communications Manager Security Features That Are Used by Cisco Unity (continued)

Security Feature	Description
Signaling encryption	Uses cryptographic methods to protect (through encryption) the confidentiality of all SCCP signaling messages that are sent between the Cisco Unity voice messaging ports and Cisco Unified CM. Signaling encryption ensures that the information that pertains to the parties, DTMF digits that are entered by the parties, call status, media encryption keys, and so on are protected against unintended or unauthorized access. This feature protects against: • Man-in-the-middle attacks that observe the information flow between Cisco Unified CM and the Cisco Unity voice messaging ports. • Network traffic sniffing that observes the signaling information flow between Cisco Unified CM and the Cisco Unity voice messaging ports.
Media encryption	Uses Secure Real Time Protocol (SRTP) as defined in IETF RFC 3711 to ensure that only the intended recipient can interpret the media streams between Cisco Unity voice messaging ports and endpoints, for example, phones or gateways. Only audio streams are encrypted. Media encryption creates a media master key pair for the devices, delivers the keys to Cisco Unity and the endpoint, and secures the delivery of the keys while the keys are in transport. Cisco Unity and the endpoint use the keys to encrypt and decrypt the media stream. This feature protects against: • Man-in-the-middle attacks that listen to the media stream between Cisco Unified CM and the Cisco Unity voice messaging ports. • Network traffic sniffing that eavesdrops on phone conversations that flow between Cisco Unified CM, the Cisco Unity voice messaging ports, and IP phones that are managed by Cisco Unified CM. Authentication and signaling encryption are required for media encryption; that is, if the devices do not support authentication and signaling encryption, media encryption cannot occur.

Note that Cisco Unified CM authentication and encryption protects only calls to Cisco Unity. Messages recorded on the message store are not protected by Cisco Unified CM authentication and encryption but can be protected by the Cisco Unity secure messaging feature.

Note The secure messaging feature is available only when Exchange is the message store.

For more information on secure messaging, see the "Securing Subscriber Messages" chapter of the *Security Guide for Cisco Unity Release 5.x (With Microsoft Exchange)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.

Authentication and encryption between Cisco Unity and Cisco Unified CM require:

- A Cisco Unified CM CTL file that lists all Cisco Unified CM servers that are entered in Cisco Unity Telephony Integration Manager (UTIM) for secure clusters.
- A Cisco Unity server root certificate for each Cisco Unity that uses authentication and/or encryption. A root certificate is valid for 20 years from the time it was created.
- Cisco Unity voice messaging port device certificates that are rooted in the Cisco Unity server root certificate and that the voice messaging ports present when registering with the Cisco Unified CM server.

The process of authentication and encryption of Cisco Unity voice messaging ports is as follows:

1. Each Cisco Unity voice messaging port connects to the TFTP server, downloads the CTL file, and extracts the certificates for all Cisco Unified CM servers.
2. Each Cisco Unity voice messaging port establishes a network connection to the Cisco Unified CM TLS port through Winsock. By default, the TLS port is 2443, though the port number is configurable.
3. Each Cisco Unity voice messaging port establishes a TLS connection to the Cisco Unified CM server, verifies the device certificate, and authenticates the voice messaging port.
4. Each Cisco Unity voice messaging port registers with the Cisco Unified CM server, specifying whether the voice messaging port will also use media encryption.

When Data Is Encrypted

When a call is made between Cisco Unity and Cisco Unified CM, the call-signaling messages and the media stream are handled in the following manner:

- If both end points are set for encrypted mode, the call-signaling messages and the media stream are encrypted.
- If one end point is set for authenticated mode and the other end point is set for encrypted mode, the call-signaling messages are authenticated, but neither the call-signaling messages nor the media stream are encrypted.
- If one end point is set for non-secure mode and the other end point is set for encrypted mode, neither the call-signaling messages nor the media stream are encrypted.

Cisco Unified Communications Manager Cluster Security Mode Settings in Cisco Unity

The Cisco Unified CM cluster security mode settings in the Cisco Unity Telephony Integration Manager (UTIM) determine how the ports handle call-signaling messages and whether encryption of the media stream is possible. Table 6-4 describes the effect of the Cluster Security Mode settings in UTIM.

Table 6-4 Cisco Unified Communications Manager Cluster Security Mode Settings for Voice Messaging Ports

Setting	Effect
Non-secure	The integrity and privacy of call-signaling messages will not be ensured because call-signaling messages will be sent as clear (unencrypted) text and will be connected to Cisco Unified CM through a non-authenticated port rather than an authenticated TLS port. The media stream is not encrypted.

Table 6-4 Cisco Unified Communications Manager Cluster Security Mode Settings for Voice Messaging Ports

Setting	Effect
Authenticated	The integrity of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port. However, the privacy of call-signaling messages will not be ensured because they will be sent as clear (unencrypted) text. The media stream is not encrypted.
Encrypted	The integrity and privacy of call-signaling messages will be ensured because they will be connected to Cisco Unified CM through an authenticated TLS port, and the call-signaling messages will be encrypted. The media stream can be encrypted. **Caution** Both end points must be registered in encrypted mode for the media stream to be encrypted. However, when one end point is set for non-secure or authenticated mode and the other end point is set for encrypted mode, the media stream will not be encrypted. Also, if an intervening device (such as a transcoder or gateway) is not enabled for encryption, the media stream will not be encrypted.

Disabling and Re-Enabling Security

The authentication and encryption features between Cisco Unity and Cisco Unified CM can be enabled and disabled by changing the Cisco Unified CM Cluster Security Mode for all Cisco Unified CM clusters to Non-Secure, and by changing the applicable settings in the Cisco Unified CM Administration.

Authentication and encryption can be re-enabled by changing the Cisco Unified CM Cluster Security Mode to Authenticated or Encrypted.

Note that after disabling or re-enabling authentication and encryption, it is not necessary to export the Cisco Unity server root certificate and copy it to all Cisco Unified CM server.

Multiple Integrations Can Have Different Security Mode Settings

When Cisco Unity is integrated with multiple Cisco Unified CM clusters, each cluster can have a different setting for Cisco Unified CM Cluster Security Mode. For example, Cluster 1 can be set to Encrypted, and Cluster 2 can be set to Non-Secure.

Settings for Individual Voice Messaging Ports

For troubleshooting purposes, authentication and encryption for Cisco Unity voice messaging ports can be individually enabled and disabled. At all other times, we recommend that the Security Mode setting for all voice messaging ports on the Ports tab be the same as the Cisco Unified CM Cluster Security Mode setting on the Servers tab.

Packetization (SCCP Integrations Only)

The Real-Time Transport Protocol (RTP) is used to send and receive audio packets over the IP network. Each discrete packet has a fixed-size header, but the packets themselves can vary in size, depending on the size of the audio stream to be transported (which varies by codec) and the packetization setting. This variable size function helps utilize network bandwidth more efficiently. Reducing the number of packets that are created per call sends fewer total bytes over the network.

Packetization is set in the Cisco Unified CM Service Parameters, in the Preferred G711 Millisecond PacketSize and Preferred G729 Millisecond PacketSize parameters. Cisco Unity supports any packet size up to 30ms for G.711 audio, and any packet size up to 60 ms for G.729a audio. The default setting is 20ms for both; there may be latency issues with lower settings.

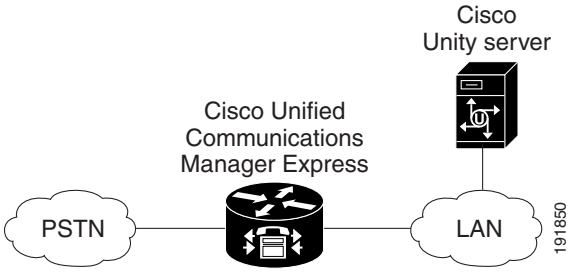
DSCP is a priority setting on each packet. DSCP helps intermediary routers manage network congestion and lets them know which packets to prioritize ahead of others. Following Cisco AVVID standards, the Cisco Unity-CM TSP marks the SCCP packets (call control) with a default DSCP value of 26 (the TOS octet is 0x68), and the RTP packets (audio traffic) with a default DSCP value of 46 (the TOS octet is 0xB8). Thus, the RTP audio packets can be assigned priority over other packets by using the router settings. Note that even though Cisco Unified CM allows you set different DSCP values, when integrated with Cisco Unity, the DSCP values set by the Cisco Unity-CM TSP always take precedence.

With each new audio stream (once per call), Cisco Unified CM tells Cisco Unity which packet size to use, and the Cisco Unity-CM TSP sets the DSCP priority for the stream. The entire stream (call) stays at the specified packet size and priority. For example, an audio stream could be broken up into packets of 30ms each. A 30ms G.729a audio stream would be 30 bytes plus the header per packet, and a 30ms G.711 stream would be 240 bytes plus the header per packet. For information on setting Cisco Unified CM Service Parameters, see the Cisco Unified CM documentation at http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html.

Integrating with Cisco Unified Communications Manager Express (by Using SCCP or SIP)

Cisco Unity supports Cisco Unified Communications Manager (CM) Express (formerly known as Cisco Unified CallManager Express) integrations through both SCCP and SIP interfaces. Figure 6-8 shows the connections.

Figure 6-8 Cisco Unity SCCP and SIP Connections to Cisco Unified Communications Manager Express Over a LAN



See Table 6-5 for information on the differences in these integration methods.

Table 6-5 Differences Between SCCP and SIP Integration Methods

Feature	SCCP	SIP
Communication method	Cisco Unity-CM TSP	SIP trunk
Failover	Supported	Not supported
Use of SCCP and SIP phones	Supported	Some SCCP phones may require use of a media termination point (MTP)
Support for Cisco Unified CM versions	All versions	Versions 5.x and later
Cisco Unified CM versions 5.x and later	Supported	Supported
Cisco Unified CM authentication and encryption	Supported	Not supported
First/last redirecting number	Supported	Supported
QOS	Supported	Supported

For information on the compatibility of Cisco Unity and Cisco Unified CM Express versions with the Cisco Unity-CM TSP and the SIP trunk, see the following documents at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html:

- *SCCP Compatibility Matrix: Cisco Unity, the Cisco Unity-CM TSP, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express*
- *SIP Trunk Compatibility Matrix: Cisco Unity and Cisco Unified Communications Manager*

For information on how to integrate Cisco Unity with Cisco Unified CM Express, see the applicable Cisco Unity integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

For more information on using the SIP protocol to integrate Cisco Unity with Cisco Unified CM Express, see the "Integrating by Using SIP" section on page 6-22.

Multiple Cisco Unified Communications Manager Express Version Support

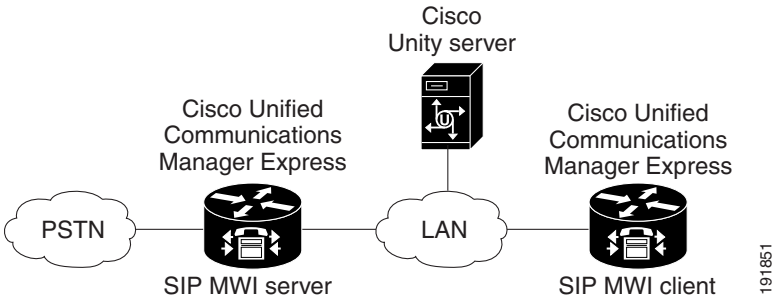
A single Cisco Unity server can support multiple versions of Cisco Unified CM Express. The version of the Cisco Unity-CM TSP or SIP trunk being used must support all versions of Cisco Unified CM Express integrated with Cisco Unity. See the following documents at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html:

- *SCCP Compatibility Matrix: Cisco Unity, the Cisco Unity-CM TSP, Cisco Unified Communications Manager, and Cisco Unified Communications Manager Express*
- *SIP Trunk Compatibility Matrix: Cisco Unity and Cisco Unified Communications Manager*

Multiple Cisco Unified Communications Manager Express Routers Integrating with a Single Cisco Unity Server

A single, centralized Cisco Unity server can be used by multiple Cisco Unified CM Express routers. This configuration requires that one Cisco Unified CM Express router be on the same LAN or WAN as the Cisco Unity server, and that this Cisco Unified CM Express router register all Cisco Unity voice messaging ports. The Cisco Unified CM Express router (the SIP MWI server) is a proxy server that relays SIP MWI messages between the Cisco Unity and all other Cisco Unified CM Express routers (the SIP MWI clients). Note that Cisco Unity voice messaging ports register with only the SIP MWI server (the Cisco Unified CM Express router that is on the same LAN as the Cisco Unity server), not with the SIP MWI clients.

Figure 6-9 Connections Between Multiple Cisco Unified CM Express Routers and a Single Cisco Unity Server

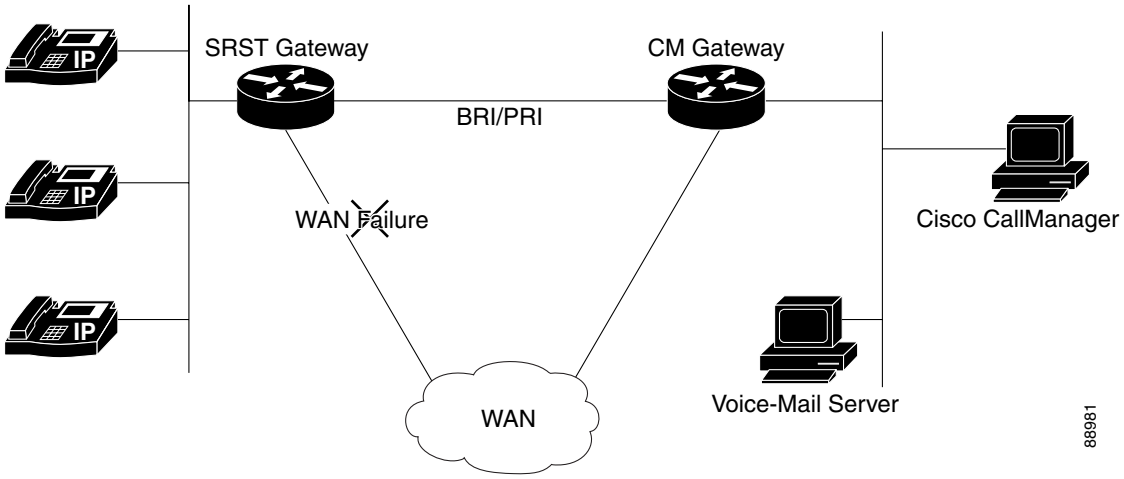


For information on configuring Cisco Unity to support multiple Cisco Unified CM Express routers, see the applicable Cisco Unity integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Integrating Cisco Unity with Cisco Survivable Remote Site Telephony (Cisco SRST)

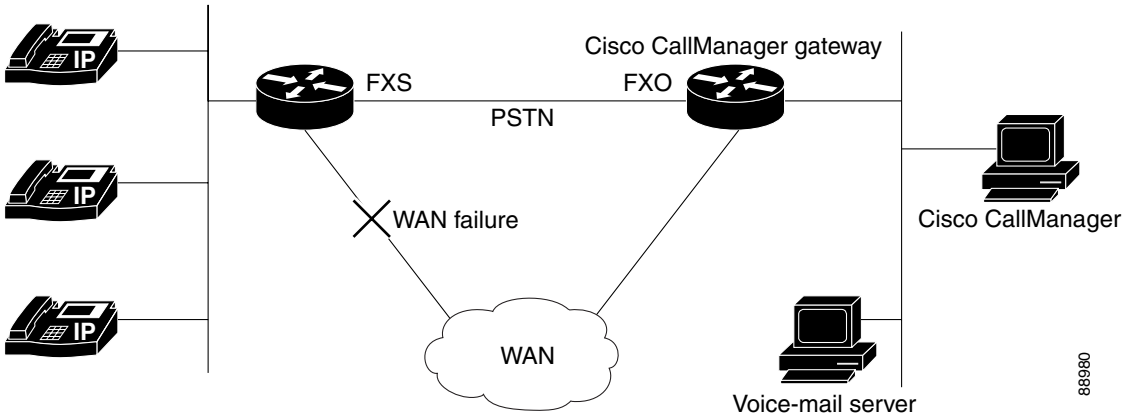
Cisco Unified Survivable Remote Site Telephony (SRST) can send and receive voice messages from Cisco Unity during Cisco Unified CM fallback. When the WAN is down and Cisco Unity has Basic Rate Interface (BRI) or Primary Rate Interface (PRI) access to the Cisco SRST system, Cisco Unity uses ISDN signaling (see Figure 6-10).

Figure 6-10 Cisco Unified Communications Manager Fallback with BRI or PRI



When the WAN is down and Cisco Unity has foreign exchange office (FXO) or foreign exchange station (FXS) access connect to a public switched telephone network (PSTN), Cisco Unity uses in-band dual tone multifrequency (DTMF) signaling (see Figure 6-11).

Figure 6-11 Cisco Unified Communications Manager Fallback with PSTN



In both configurations, phone message buttons remain active and calls to busy or unanswered numbers are forwarded to Cisco Unity. The installer must configure access from the dial peers to the voice-mail system, and establish routing to Cisco Unity for busy and unanswered calls and for the message button.

If Cisco Unity is accessed over FXO or FXS, you must configure instructions (DTMF patterns) for Cisco Unity so it can access the correct voice-mail system mailbox.

When using Cisco Unified SRST with Cisco Unity, the integration has the following limitations during a WAN outage:

Call forward to busy greeting	When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call is forwarded from a branch office to Cisco Unity, the busy greeting cannot play.

Call forward to internal greeting	When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call is forwarded from a branch office to Cisco Unity, the internal greeting cannot play. Because the PSTN provides the calling number of the FXO line, the caller is not identified as a subscriber.
Call transfers	Because an access code is needed to reach the PSTN, call transfers from Cisco Unity to a branch office will fail.
Identified subscriber messaging	When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a subscriber at a branch office leaves a message or forwards a call, the subscriber is not identified. The caller appears as an unidentified caller.
Message waiting indication	MWIs are not updated on branch office phones, so MWIs will not correctly reflect when new messages arrive or when all messages have been listened to. We recommend resynchronizing MWIs after the WAN link is reestablished.
Message notification	Because an access code is needed to reach the PSTN, message notifications from Cisco Unity to a branch office will fail.
Routing rules	When the Cisco Unified SRST router uses FXO/FXS connections to the PSTN and a call arrives from a branch office to Cisco Unity (either a direct or forwarded call), routing rules will fail.

When the Cisco Unified SRST router uses PRI or BRI connections, the caller ID for calls from a branch office to Cisco Unity may be the full number (exchange plus extension) provided by the PSTN and therefore may not match the extension of the Cisco Unity subscriber. In this case, you can let Cisco Unity recognize the caller ID by using alternate extensions or by using extension remapping. For information on extension remapping, see the "Remapping Extension Numbers" section of the "Managing System-Wide Settings" chapter in the applicable *System Administration Guide for Cisco Unity Release 5.x*, available at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_maintenance_guides_list.html.)

When using Cisco Unified SRST, Redirected Dialed Number Information Service (RDNIS) must be supported.

For information on setting up Cisco Unified SRST routers, see the "Integrating Voice Mail with Cisco Unified SRST" section of the *Cisco Unified SRST System Administrator Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html.

Impact of Non-Delivery of RDNIS on Voice Mail Calls Routed via AAR

RDNIS needs to be supported when using Automated Alternate Routing (AAR).

AAR can route calls over the PSTN when the WAN is oversubscribed. However, when calls are rerouted over the PSTN, RDNIS can be affected. Incorrect RDNIS information can affect voice mail calls that are rerouted over the PSTN by AAR when Cisco Unity is remote from its messaging clients. If the RDNIS information is not correct, the caller will not reach the mailbox of the dialed user but will instead receive the automated attendant prompt, and the caller might be asked to reenter the extension number of the party they want to reach. This behavior is primarily an issue when the telephone carrier is unable to ensure RDNIS across the network. There are numerous reasons why the carrier might not be able to ensure that RDNIS is properly sent. Check with your carrier to determine whether it provides guaranteed RDNIS delivery end-to-end for your circuits. The alternative to using AAR for oversubscribed WANs is simply to let callers hear reorder tone in an oversubscribed condition.

Integrating Cisco Unity with Cisco Unified Communications Manager Express in SRST Mode

Cisco Unity supports a topology with centralized call processing and distributed messaging, in which your Cisco Unity server is located at a remote site or branch office and registered with the Cisco Unified CM at a central site.

When the WAN link fails, the phones fall back to the Cisco Unified CM Express-as-SRST device. Cisco Unity can also fall back to the Cisco Unified CM Express-as-SRST device, which lets users at the remote site access their voice messages and see message waiting indicators (MWIs) during a WAN outage. Note that MWIs must be resynchronized from the Cisco Unity server whenever a failover happens from Cisco Unified CM to Cisco Unified CM Express-as-SRST or vice versa.

For information on setting up this configuration, see the *Integrating Cisco Unity with Cisco Unified CME-as-SRST* application note at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/prod_troubleshooting_guides_list.html.

Integrating by Using SIP

SIP (Session Initiation Protocol) is the Internet Engineering Task Force standard for multimedia calls over IP. SIP is a peer-to-peer, ASCII-based protocol that uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more end points. A SIP network uses the following components:

SIP proxy server	The proxy server is an intermediate device that receives SIP requests from a client and then forwards the requests on behalf of the client. Proxy servers receive SIP messages and forward them to the next SIP server in the network. Proxy servers can provide functions such as authentication, authorization, network access control, routing, reliable request retransmission, and security.
Redirect server	Provides information to the client about the next hop or hops that a message should take. The client then contacts the next hop server or user-agent server directly.
Registrar server	Processes requests from user agent clients for registration of their current location. Registrar servers are often installed on the redirect or proxy server.
Phones	Can act as either a server or client. Softphones (PCs that have phone capabilities installed) and Cisco SIP IP phones can initiate SIP requests and respond to requests.
Gateways	Provide call control. Gateways provide many services; the most common is a translation function between SIP call endpoints and other terminal types. This function includes translation between transmission formats and between communications procedures. In addition, the gateway translates between audio and video codecs, and performs call setup and clearing on both the LAN side and the switched-circuit network side.

Cisco Unity accepts calls from a proxy server. Cisco Unity relies on a proxy server or call agent to authenticate calls.

SIP uses a request/response method to establish communications between various components in the network and to ultimately establish a conference (call or session) between two or more endpoints. A single call may involve several clients and servers.

Users in a SIP network are identified by:

- A unique phone or extension number.

- A unique SIP address, which is similar to an e-mail address and uses the format sip:<userID>@<domain>. The user ID can be either a user name or an E.164 address.

When a user initiates a call, a SIP request typically goes to a SIP server (either a proxy server or a redirect server). The request includes the caller's address (From) and the address of the called party (To).

SIP messages are in text format using ISO 10646 in UTF-8 encoding (like HTML). In addition to the address information, a SIP message contains a start-line specifying the method and the protocol, a number of header fields specifying call properties and service information, and an optional message body which can contain a session description.

Supported SIP Integrations

Cisco Unity currently supports the following SIP integrations:

- SIP trunks to selected versions of Cisco Unified Communications Manager and Cisco Unified Communications Manager Express. For a list of Cisco Unified CM and Cisco Unified CM Express versions supported as SIP trunks, see *SIP Trunk Compatibility Matrix: Cisco Unity and Cisco Unified Communications Manager* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_device_support_tables_list.html.
- Cisco SIP Proxy Server (CSPS). However, CSPS is being phased out, so using it for a SIP integration is not encouraged.

Third-party SIP trunks are currently not supported.

For more information on configuring SIP trunks between Cisco Unity and Cisco Unified CM or Cisco Unified CM Express, see the applicable SIP trunk integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Cisco Unity Failover with SIP Trunks

Cisco Unity failover is not supported with either the Cisco Unified CM SIP trunk integration or the Cisco Unified CM Express SIP trunk integration. If Cisco Unity failover is a requirement, you must use the Skinny Call Control Protocol (SCCP) integration with Cisco Unified CM. A customer can continue to use SIP phones when integrating with Cisco Unified CM using the SCCP integration. Once a call is established between a SIP phone and Cisco Unity, which is using Skinny, the RTP session between the two endpoints will work properly.

Note that Cisco Unity failover is not supported for Cisco Unified CM Express using either the SIP trunk integration or SCCP integration.

SIP Compliance

For information on Cisco Unity compliance with the SIP standard, see *SIP Compliance for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_white_papers_list.html.

Integrating with Circuit-Switched Phone Systems by Using PIMG or TIMG Units

Cisco Unity can integrate with circuit-switched phone systems by using the Dialogic Media Gateway (PIMG or TIMG units) between circuit-switched phone systems and IP networks.

For a list of circuit-switched phone systems currently supported with Cisco Unity using PIMG and TIMG integrations, see the "Supported Phone System Integrations" section of *Supported Hardware and Software, and Support Policies for Cisco Unity Release 5.x*. at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

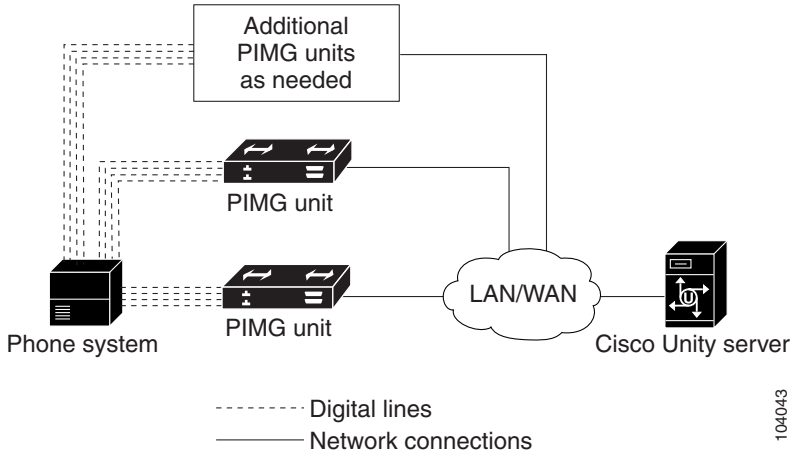
Description of PIMG Integrations

The PIMG integration uses one or more PIMG units between the circuit-switched phone systems and IP network. On the circuit-switched phone system side, there are both digital (feature-set) and analog interfaces; the interface used will depend on the phone system to which Cisco Unity is connected. On the IP side, there is a SIP interface, which is how Cisco Unity communicates with the PIMG gateway. To Cisco Unity, the integration is essentially a SIP integration. Cisco Unity communicates with the PIMG gateway over the IP network using SIP and RTP protocols. The PIMG gateway communicates with the circuit-switched phone system over the phone network using phone system-specific protocols (digital, analog, serial). Note that there are digital integrations for circuit-switched phone systems from several vendors, which are tighter integrations than the Cisco Unity analog integrations using voice cards.

Digital Integration with Digital PIMG Units

The phone system sends call information, MWI requests, and voice connections through the digital lines, which connect the phone system to the PIMG units. The PIMG units communicate with the Cisco Unity server through the LAN or WAN by using Session Initiation Protocol (SIP). Figure 6-12 shows the connections for a digital integration by using digital PIMG units.

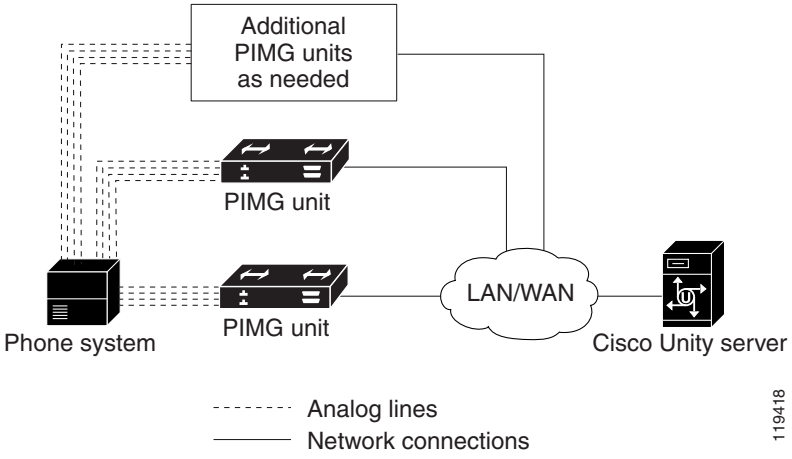
Figure 6-12 Connections for a Digital Integration by Using Digital PIMG Units



DTMF Integration with Analog PIMG Units

The phone system sends call information, MWI requests, and voice connections through the analog lines, which connect the phone system to the PIMG units. The PIMG units communicate with the Cisco Unity server through the LAN or WAN by using Session Initiation Protocol (SIP). Figure 6-13 shows the connections for a DTMF integration by using analog PIMG units.

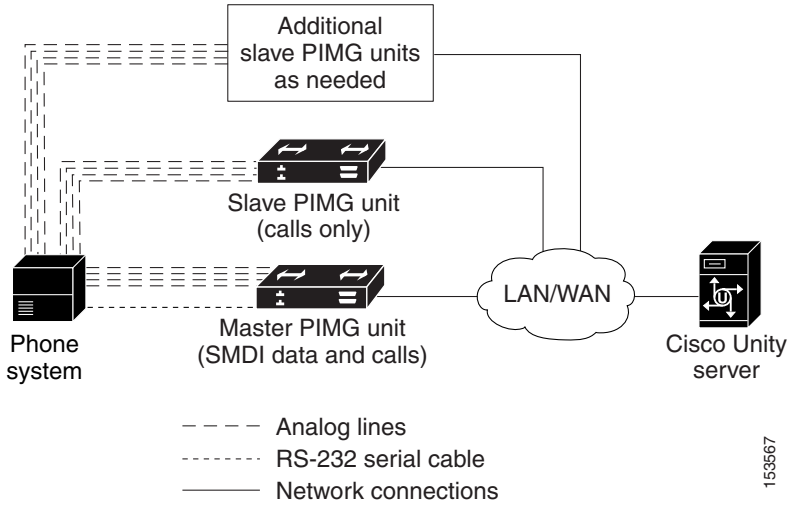
Figure 6-13 Connections for a DTMF Integration by Using Analog PIMG Units



Serial (SMDI, MCI, or MD-110) Integration with Analog PIMG Units

The phone system sends call information and MWI requests through the data link, which is an RS-232 serial cable that connects the phone system and the master PIMG unit. Voice connections are sent through the analog lines between the phone system and the PIMG units. The PIMG units communicate with the Cisco Unity server through the LAN or WAN by using Session Initialization Protocol (SIP). Figure 6-14 shows the connections for a serial integration by using analog PIMG units.

Figure 6-14 Connections for a Serial (SMDI, MCI, or MD-110) Integration by Using Analog PIMG Units



Note When you use multiple PIMG units, one PIMG unit must be designated the master PIMG unit, which will be connected to the serial cable. It is not possible to "daisy chain" the serial ports on the PIMG units.

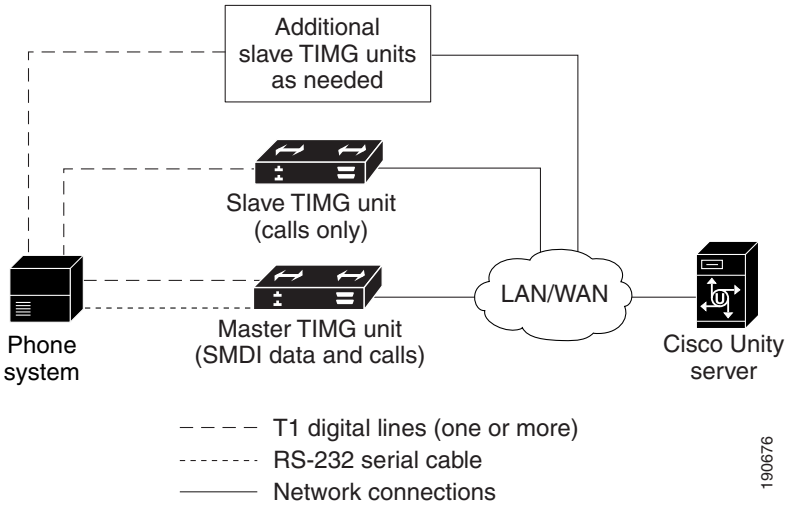
You can add a secondary master PIMG unit to an integration. For details, see the *PIMG Integration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Description of TIMG Integrations

The TIMG integration uses one or more TIMG units between circuit-switched phone systems and IP networks. On the circuit-switched phone system side, there is a T1-CAS interface. On the IP side, there is a SIP interface, which is how Cisco Unity communicates with the TIMG unit. To Cisco Unity, the integration is essentially a SIP integration. Cisco Unity communicates with the TIMG unit over the IP network using SIP and RTP protocols. The TIMG unit communicates with the circuit-switched phone system over the phone network using serial protocols (SMDI, MCI, or MD-110).

The phone system sends call information and MWI requests through the data link, which is an RS-232 serial cable that connects the phone system and the master TIMG unit. Voice connections are sent through the T1 digital lines between the phone system and the TIMG units. The TIMG units communicate with the Cisco Unity server through the LAN or WAN by using SIP. Figure 6-15 shows the connections.

Figure 6-15 Connections for an Integration by Using TIMG Units



Setup and Configuration

For PIMG/TIMG setup and configuration, the installer does the following steps as documented in the applicable integration guide:

1. Configure the phone system.
2. Configure the PIMG/TIMG units. PIMG/TIMG settings are somewhat phone system-specific, but less so than phone system configuration.
3. Configure Cisco Unity for the integration.

For information on configuring the phone system, PIMG/TIMG units, and Cisco Unity, see the applicable Cisco Unity integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Firmware Updates

Note that when receiving shipment of PIMG or TIMG units, it may be necessary to update the firmware on the units. The PIMG/TIMG Admin interface provides a simple method to update the firmware files. Firmware updates are available on CCO (Cisco Connection Online). See the applicable integration guide or check for the latest firmware updates on the Cisco Unity PIMG page at http://www.cisco.com/cgi-bin/tablebuild.pl/unity-PIMG.

Serial Integrations

Cisco Unity supports the following serial protocols:

- SMDI
- MCI
- MD-110

When older versions of Cisco Unity integrated with a circuit-switched phone system by using a serial integration, if the phone system did not use standard serial packets (such as SMDI or MCI), it was possible to adjust the serial packet definitions by using Cisco Unity .avd files. Unfortunately, PIMG/TIMG units do not allow customization of serial packet definitions, so only phone systems that comply with the standards will work.

The serial port on PIMG unit was originally designed as a management port rather than as a standard RS-232 serial port. Consequently, a custom serial cable (which is available from Cisco) is necessary for the datalink between the phone system and the master PIMG unit. The pinout of the custom serial cable is available in the *PIMG Integration Guide* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Increasing Port Capacity

PIMG units have eight ports. To increase system port capacity, multiple PIMG units can be stacked. For example, if 32 ports are needed, 4 PIMG units can be stacked. When stacking two or more PIMG units, each PIMG unit must communicate with Cisco Unity by using a different IP port. The first PIMG talks to Cisco Unity port 5060, and each successive unit uses the next higher port (5061, 5062, and so on).

TIMG units, which integrate with circuit-switched phone systems that support T1-CAS, have 24 T1 ports per span in a single rack-optimized unit. Single span and dual span TIMG units are available.

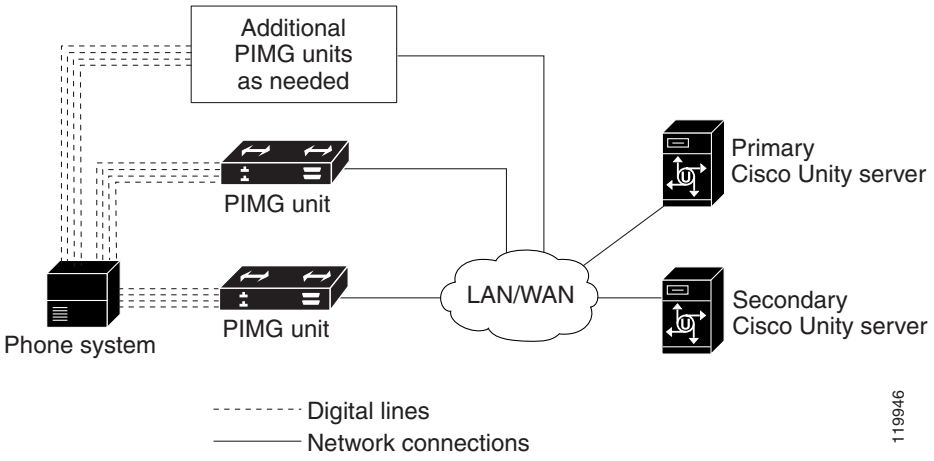
Cisco Unity Failover

PIMG/TIMG integrations support Cisco Unity failover. Configuration changes are required both for the PIMG/TIMG units and for the Cisco Unity servers, as described in the applicable integration guide. The IP addresses of both Cisco Unity servers must be entered in each PIMG/TIMG unit. The settings in UTIM (Cisco Unity Telephony Integration Manager) for the secondary Cisco Unity server must match those of the primary Cisco Unity server. This includes the integration number, which may vary.

Cisco Unity failover is different for PIMG/TIMG integrations in that a Cisco Unity server cannot explicitly tell a PIMG unit whether it is active and should receive calls. Rather, PIMG/TIMG units will infer the active server based upon which Cisco Unity server responds to incoming calls and upon keepalive messages received from the primary Cisco Unity server. When the primary Cisco Unity server is active, the PIMG/TIMG units will send calls to it. If the primary server does not answer or send keepalive messages, the PIMG/TIMG units will pull the call back and send it to the secondary Cisco Unity server. When the secondary Cisco Unity server answers, the PIMG/TIMG units will assume the secondary is the active server, and route all further calls to the secondary server. While the secondary Cisco Unity server is active, the PIMG/TIMG units will send periodic keepalive messages to the primary server. When the primary Cisco Unity server responds, the PIMG/TIMG units will route calls to the primary server.

The connections for a PIMG integration with Cisco Unity failover are shown in Figure 6-16.

Figure 6-16 Connections for a PIMG Integration with Cisco Unity Failover



Cisco Unity Failback

Before failing back from the secondary server to the primary server, you must first disable automatic failover. Otherwise, the PIMG/TIMG units will continue to send INVITE messages to the secondary server for new calls, which will cause failover to occur before failback has completed. Do the following procedure when initiating failback from the secondary Cisco Unity server to the primary server.

To Initiate Failback from a Secondary Cisco Unity Server to the Primary Server

Step 1 On the Windows Start menu, click **Programs > Cisco Unity > Failover Monitor**.

Step 2 Click **Configure**.

Step 3 Uncheck the **Force Failover If Call Arrives on Inactive Secondary** check box, and click **OK**.

Step 4 Initiate failback, and wait at least 10 seconds.

Step 5 Re-enable automatic failover.

Multiple Integration Support/Branch Office Consolidation

Cisco Unity does not limit the number of PIMG integrations. It is possible, though not practical, to create 144 separate phone system integrations with one port each for a total of 144 ports and 144 PIMG units.

PIMG unit can be placed across a WAN to support circuit-switched phone systems at remote branch office sites. Cisco Unity would be placed at a centralized headquarters, for example, and support circuit-switched phone systems both at headquarters and at branch office sites.

Assuming there are four phone systems from four different manufacturers (for example, Nortel, Avaya, NEC, and Siemens), four different integrations will be created on the Cisco Unity server to support the four phone systems. Across those four integrations, Cisco Unity can support 144 ports. For example:

- At the Seattle site, 15 PIMG units can be stacked to support 122 ports.
- At the New York site, two PIMG units can be stacked to support 16 ports.
- At the Tokyo site, one PIMG unit can be used to support four ports.
- At the Dallas site, one PIMG unit can be used to support two ports.

Even though the PIMG units come with eight ports, fewer than eight ports can be used on each unit.

If PIMG units will be placed across a WAN to support remote phone systems, proper codec selection, bandwidth capacity planning, and QOS planning are required. Both the G729a and G711 codec are supported by PIMG units and by Cisco Unity. Because PIMG units are Dialogic rather than Cisco devices, the use of location-based CAC is not applicable. The following network and bandwidth requirements are required when placing the PIMG across a WAN:

- For G.729a codec formatting, a minimum of 32.76 Kbps (assumes Ethernet, payload of 20 bytes, 5 percent overhead) guaranteed bandwidth for each voice messaging port
- For G.711 codec formatting, a minimum of 91.56 Kbps (assumes Ethernet, payload of 160 bytes, 5 percent overhead) guaranteed bandwidth for each voice messaging port
- No network devices that implement network address translation (NAT)

Note When the G.729a codec is used, Cisco Unity cannot perform silence detection. Using this codec may result in messages that have long trailing silence or that are entirely silent.

When placing PIMG units across a WAN, prioritize your call control and media traffic via proper QOS traffic, marking for voice traffic originating on the PIMG units. Set the Call Control QOS Byte and RTP QOS Byte on PIMG units to the following values:

Call Control QOS Byte	• PIMG units connect only to a LAN: 0 (CSCsb96387) • PIMG units connect to a WAN: 104
RTP QOS Byte	• PIMG units connect only to a LAN: 0 (CSCsb96387) • PIMG units connect to a WAN: 184

Note that the Call Control and RTP QOS byte parameters on PIMG units define a decimal value that represents QOS bit flags. These values can be interpreted as either IPv4 TOS or Differentiated Services Codepoint (DSCP). For more details, see the applicable PIMG User Guide.

Support for integrations with multiple circuit-switched phone systems up to a maximum of 144 ports allows Cisco Unity to consolidate multiple branch office sites into one centralized Cisco Unity server. For more information, see the "Integrating with Multiple Phone Systems" section on page 6-30.

Integrating with Multiple Phone Systems

Beginning with Cisco Unity 5.0(1), Cisco Unity supports as many integrations as necessary up to 144 ports. For example, you can create 144 integrations, each with only one port, for a total of 144 ports.

Requirements for Integrations with Multiple Phone Systems

Cisco Unity has the following requirements for multiple phone system integrations:

- All phone system and Cisco Unity server requirements have been met. See the applicable Cisco Unity integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.
- There must be an adequate number of voice messaging ports on the Cisco Unity server to connect to the phone systems. This number must not exceed the number of ports that are enabled by the Cisco Unity license files.
- For a single Cisco Unity server (or a failover pair), all extensions must be unique. The dial plans for the phone systems must not overlap.

  If overlapping dial plans cannot be avoided, you must install a Cisco Unity server for each phone system, digitally network the servers, and set up dialing domains to accommodate the overlapping dial plans. See the applicable *Networking Guide for Cisco Unity Release 5.x* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.
- For limitations on combinations for multiple phone system integrations, see the "Combination Limitations for Multiple Phone System Integrations" section in the *Multiple Phone System Integration Guide for Cisco Unity 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Using SCCP Phone Systems with Other Integrations

The SCCP phone system type includes integrations through SCCP (Skinny Call Control Protocol) with Cisco Unified Communications Manager and with Cisco Unified Communications Manager Express.

For Cisco Unified CM phone systems, you can add Cisco Unified CM clusters in UTIM as separate phone system integrations or as new clusters to an existing Cisco Unified CM integration. For more information, see the "Creating an Integration with a Second Cluster of Cisco Unified Communications Manager" section in the applicable Cisco Unified CM integration guide at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_installation_and_configuration_guides_list.html.

Cisco Unity can integrate with Cisco Unified CM Express in SRST mode. For details, see the *Integrating Cisco Unity with Cisco Unified CME-as-SRST* application note at http://www.cisco.com/en/US/products/sw/voicesw/ps4625/prod_troubleshooting_guides_list.html.

Notes for PIMG Integrations

There is no limit on the number of PIMG units that you can use. If you want to connect PIMG units to different phone systems, add the PIMG units that are connected to one phone system to one integration, and add the PIMG units that are connected to a different phone system to another integration.

Optional Integration Features

See the following sections:

- Alternate Extensions, page 6-32
- Alternate MWIs, page 6-33

Alternate Extensions

In addition to the primary extension that you specify for each subscriber, you can assign a subscriber up to nine alternate extensions. (The primary extension is the one that you assign to each subscriber when you create his or her subscriber account; in the Cisco Unity Administrator, it is listed on the Subscribers > Subscribers > Profile page.)

Reasons to Use Alternate Extensions

There are several reasons that you may want to specify alternate extensions for subscribers. For example, if you have more than one Cisco Unity server that accesses a single, corporate-wide directory, you may want to use alternate extensions to simplify addressing messages to subscribers at the different locations. With alternate extensions, the number that a subscriber uses when addressing a message to someone at another location can be the same number that the subscriber dials when calling. You may also want to use alternate extensions to:

- Handle multiple line appearances on subscriber phones.
- Offer easy message access on direct calls from a cell phone, home phone, or phone at an alternate work site (assuming that the phone number is passed along to Cisco Unity from these other phone systems). In addition, when such phones are used as alternate extensions, and are set to forward to Cisco Unity, callers can listen to the subscriber greeting, and leave messages for the subscriber just as they would when dialing the primary extension for the subscriber.
- Enable URL-based extensions in Cisco Unity for an integration with a SIP phone system.

To reduce the number of requests from subscribers who want alternate extensions set up for multiple cell phones, home phones, and other phones, give subscribers class of service (COS) rights to specify their own set of alternate extensions. (In the Cisco Unity Administrator, see the Subscribers > Class of Service > Profile page.) With proper COS rights, a subscriber can specify up to five alternate extensions in the Cisco Unity Assistant in addition to the nine that you can specify on the Subscribers > Alternate Extensions page in the Cisco Unity Administrator.

How Alternate Extensions Work

Before you set up alternate extensions, review the following list for information on how alternate extensions work:

- Alternate extensions cannot exceed 30 characters in length. By default, each administrator-defined alternate extension must be at least 3 characters in length, while subscriber-defined alternate extensions must be at least 10 characters.

  You can use the Advanced Settings tool in Tools Depot to specify:

  - A minimum extension length for the extensions entered in the Cisco Unity Administrator. See the Administration—Set the Minimum Length for Locations setting.

  - A minimum extension length for the extensions entered in the Cisco Unity Assistant. See the Administration—Set the Minimum Length for Subscriber-Defined Alternate Extensions setting.

  See the Advanced Settings Tool Help for details on using the settings.

- You can control whether subscribers can use the Cisco Unity Assistant to view the alternate extensions that you specify in the Cisco Unity Administrator. To do so, see the Subscribers > Class of Service > Profile page. The Subscriber-Defined Alternate Extension table displays the alternate extensions that the subscriber adds.
- Neither the Cisco Unity Administrator nor the Cisco Unity Assistant will accept an extension that is already assigned to another subscriber (either as a primary or alternate extension), or to a public distribution list, call handler, directory handler, or interview handler. Cisco Unity verifies that each alternate extension is unique—up to the dialing domain level, if applicable—before allowing either an administrator or a subscriber to create it.
- All alternate extensions use the same transfer settings as the primary extension.
- In many cases, Cisco Unity can activate a message waiting indicator (MWI) for an alternate extension. However, depending on the phones and phone systems involved, some additional phone system programming may be required to set this up.

Alternate MWIs

You can set up Cisco Unity to activate alternate MWIs when you want a new message for a subscriber to activate the MWIs at up to 10 extensions. For example, a message left at extension 1001 can activate the MWIs on extensions 1001 and 1002.

Cisco Unity uses MWIs to alert the subscriber to new voice messages. MWIs are not used to indicate new e-mail, fax, or return receipt messages.

In Cisco Unified Communications Manager integrations, you can also use the alternate MWI feature to activate MWIs on a non-integrated phone system that can send and receive information from Cisco Unity over an RS-232 serial cable.

Setting Up Alternate MWIs for Extensions on the Same Phone System

Cisco Unity can activate alternate MWIs for extensions on the same phone system. Depending on the phones and phone systems, some additional phone system programming may be necessary. Refer to the documentation for the phone system.

MWIs for Extensions on a Non-Integrated Phone System

Cisco Unity can activate MWIs on a phone system that is not integrated with Cisco Unity and that is not part of a two phone system integration (referred to here as a non-integrated phone system). MWI activation requests are sent through an RS-232 serial cable. Calls to subscribers that come from the non-integrated phone system are routed through the gateway to Cisco Unified Communications Manager.

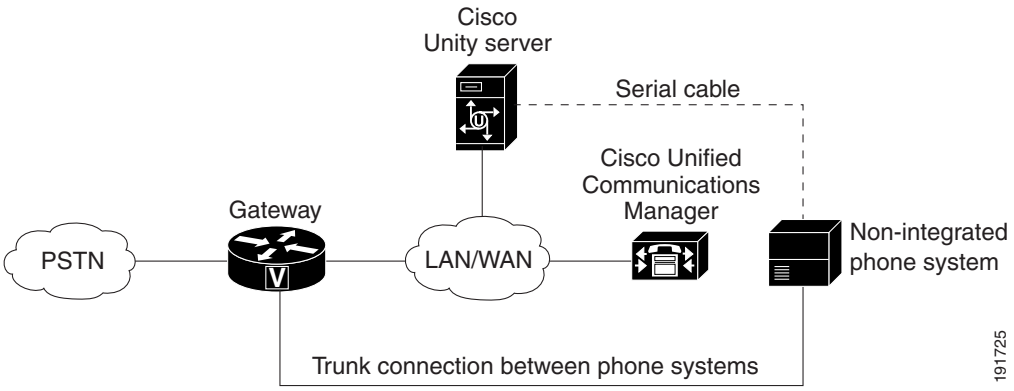
For this method, you must set up:

- A trunk connection between Cisco Unified CM and the non-integrated phone system through a gateway.

- The unique subscriber extensions on the non-integrated phone system to forward on no answer to the corresponding phantom extensions on Cisco Unified CM.
- The Switch.ini file (phone system configuration file) to enable Cisco Unity access through the serial cable for turning alternate MWIs on and off.
- An RS-232 serial cable between a Cisco Unity serial port and the non-integrated phone system serial port to send alternate MWI activation requests.
- The Cisco Unity serial configuration file, if the non-integrated phone system uses a serial configuration different from the default serial configuration used by Cisco Unity.

Figure 6-17 shows the connections via a serial cable between a Cisco Unified CM integration and a non-integrated phone system.

Figure 6-17 Connection for Sending Alternate MWIs via a Serial Cable to a Non-Integrated Phone System from a Cisco Unified Communications Manager Integration



Centralized Voice Messaging

Cisco Unity supports centralized voice messaging by supporting various inter-phone system networking protocols including, for example, proprietary protocols such as Avaya DCS, Nortel MCDN, or Siemens CorNet, and standards-based protocols such as QSIG or DPNSS.

When discussing phone systems involved in centralized voice messaging, there are essentially two types:

Message Centre PINX	The phone system hosts the voice messaging system (the phone system is directly connected to the voice messaging system).
Subscriber PINX	The phone system is remote from the voice messaging system (the phone system is not directly connected to the voice messaging system).

Centralized voice messaging provides voice messaging services to all subscribers in a networked phone system environment. Cisco Unity can be hosted on a message centre PINX and provide voice messaging services to all subscribers in an enterprise assuming the message centre PINX and all subscriber PINX phone systems are properly networked.

For a centralized voice messaging configuration to exist, a suitable inter-phone system networking protocol must exist to deliver a minimum level of feature support, such as:

- Message waiting indication (MWI).
- Transfer, which ensures that the correct calling/called party ID is delivered to the voice messaging system.
- Divert, which ensures that the correct calling/called party ID is delivered to the voice messaging system.

Other features may be required depending on how the voice messaging system is to be used (for example, if it is also serving as an automated attendant then Path-Replacement will be needed as this feature will prevent calls from hair-pinning).

Not all phone systems can serve as a message centre PINX. In this case, customers may wish to consider relocating Cisco Unity to Cisco Unified Communications Manager and have Cisco Unified CM act as the message centre PINX with the circuit-switched phone system now acting as the subscriber PINX.

For information on configuring Cisco Unity in a centralized voice messaging environment to be hosted on Cisco Unified CM serving as the message centre PINX, see the following:

- The application note *Cisco CallManager 4.1-Voicemail Interoperability: Cisco Unity 4.0(4) with Cisco CallManager 4.1(2) Configured as Message Center PINX Using Cisco Catalyst 6608 T1 Q.SIG with MGCP* at http://www.cisco.com/application/pdf/en/us/guest/products/ps5820/c1072/ccmigration_09186a00803cad8f.pdf.
- The applicable application note for configuring QSIG trunks between Cisco Unified Communications Manager and various circuit-switched phone systems on the Cisco Interoperability Portal at http://www.cisco.com/en/US/netsol/ns728/networking_solutions_products_generic_content0900aecd805b561d.html.

Note that if customers are deploying centralized voice messaging with Cisco Unity and a circuit-switched phone system, it is up to the customer to determine whether the circuit-switched phone system can serve as a message center PINX on which Cisco Unity can be hosted. If so, the customer should also confirm support for the desired features, for example, MWIs, transfer, divert, and path-replacement.

Inter-cluster trunks between Cisco Unified CM clusters can be QSIG enabled by using the Annex M.1 feature, which allows Cisco Unity to integrate with a single Cisco Unified CM cluster. Ports in the cluster with which Cisco Unity is integrated can be dedicated to turning MWIs on and off for phones in other clusters.

CHAPTER 7

Cisco Unity Failover and Standby Redundancy

See the following sections:

- Comparison of Cisco Unity Failover and Standby Redundancy, page 7-1
- Failover, page 7-1
- Standby Redundancy, page 7-2

Comparison of Cisco Unity Failover and Standby Redundancy

Cisco Unity failover provides system-malfunction failover within a data center. Failover consists of two servers, a primary and a secondary. In general, the primary server is active and taking calls, while the secondary is inactive and not taking calls. Any changes to subscriber or configuration data on the primary server are automatically replicated to the secondary server. If the primary server stops functioning for some reason, the secondary server automatically becomes the active server and starts taking calls. The primary server temporarily becomes inactive.

Cisco Unity standby redundancy provides disaster-recovery failover across geographic locations. There are still two servers, a primary and a secondary, but they are installed in separate data centers, commonly in separate cities. If the data center in which the primary server is installed is affected by a natural disaster or other catastrophe, someone in (or with remote access to) the disaster-recovery facility manually activates the secondary server, and the secondary server begins taking calls.

For more information on how failover and standby redundancy work, see the "About Cisco Unity Failover" chapter in the applicable *Failover Configuration and Administration Guide for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html.

Failover

For a list of the requirements for a failover system, see the "Requirements for Cisco Unity Failover" section in the *System Requirements for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Configuring Failover When Cisco Unity Servers Are Separated by a Firewall

Revised May 6, 2008

When Exchange is the message store, you can separate Cisco Unity primary and secondary servers by a firewall. When IBM Lotus Domino is the message store, the primary and secondary servers cannot be separated by a firewall.

If the system includes a Cisco Unity voice recognition server, the primary and secondary Cisco Unity servers must be on the same side of the firewall as the Cisco Unity voice recognition server.

For additional requirements, see the "Failover Requirements for Separating Cisco Unity Servers by a Firewall" in the *System Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Installing Exchange 2003 on the Cisco Unity Secondary Server in a Voice Messaging Configuration with Failover

When Cisco Unity failover is installed in a Voice Messaging configuration, Exchange Server 2003 can be installed on the secondary server instead of on a separate, third server. Requirements for this configuration are listed in the "Requirements When the Message Store Is Installed on the Secondary Server" section of the *System Requirements for Cisco Unity* Release 5.0 at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Requirements for Spanning a Cisco Unity Failover Pair Across Redundant Data Centers

Revised May 6, 2008

Some customers maintain redundant data centers that are so well connected that they essentially form a single LAN. For these customers, failover may be a more suitable configuration than standby redundancy. For detailed requirements for this configuration, see the section "Failover Requirements for Separating Cisco Unity Servers by a WAN" in the *System Requirements for Cisco Unity* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Standby Redundancy

Note the following about a Cisco Unity system configured for standby redundancy:

- The standby redundancy configuration requires a minimum available bandwidth of 100 Mb/second between the data centers in which the Cisco Unity primary and secondary servers are installed. This is because of two bandwidth spikes, one caused by SQL Server, the other by Cisco Unity:
  - Once daily (by default at 2:00 a.m.), SQL Server replicates data from the active server to the inactive server.
  - Cisco Unity periodically replicates WAV files of voice names, greetings, call handlers, and interview handlers from the active server to the inactive server.
- If something happens to the data center in which the Cisco Unity server is installed, the customer must have:
  - A way to reroute call traffic to the data center in which the secondary server is installed.

  - Sufficient bandwidth for call traffic to the data center in which the secondary server is installed.
- Automatic failover must be disabled when Cisco Unity standby redundancy is configured. Therefore, if the primary server becomes unavailable, the customer must manually make the secondary server active before it begins taking calls.

For a list of the requirements for standby redundancy, see the "Requirements for Standby Redundancy" section in the *System Requirements for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.

Installing Exchange 2003 on the Cisco Unity Primary Server in a Standby Redundancy Configuration

When Cisco Unity is installed in a standby redundancy configuration, Exchange Server 2003 can be installed on the primary server instead of on a separate, third server. This reduces the number of servers required for a standby redundancy configuration, and also allows Cisco Unity and Exchange to be in the same data center except when the secondary server is active.

When the secondary Cisco Unity server is active, the primary server, on which Exchange is installed, is probably completely unavailable, which means that Exchange is also unavailable. The secondary Cisco Unity server answers calls, allows outside callers to look up subscriber extensions, and records voice messages. However, subscribers who check their voice messages hear the Unity Messaging Repository (UMR) conversation. This conversation explains that their Exchange server is not available, and lets them access voice messages that were sent after the primary Cisco Unity server became unavailable. Any voice messages sent after the primary became unavailable are stored in the UMR on the secondary Cisco Unity server. When the primary Cisco Unity server is active again and Exchange on the primary is available again, the voice messages stored in the UMR are routed to the subscriber mailboxes.

Caution If the message store is already installed on a separate platform, do not reconfigure the existing Cisco Unity system to move Exchange to the primary Cisco Unity server. Otherwise, the Cisco Unity standby redundancy system will not be supported. Only new installations of Cisco Unity with standby redundancy can be configured with Exchange on the primary server.

Note This configuration is not yet documented in *System Requirements for Cisco Unity Release 5.0*, in the *Failover Configuration and Administration Guide for Cisco Unity Release 5.x*, or in the Cisco Unity installation guide. When installing Cisco Unity in this configuration, use the *Installation Guide for Cisco Unity Release 5.x in a Voice Messaging Configuration with Microsoft Exchange (With Failover Configured)*, but install Exchange on the primary server instead of on the secondary or on a separate server. You must install software on the primary server first because when you install Exchange administration software on the secondary server, the full version of Exchange must already be present in the environment.

- This configuration is supported only when Cisco Unity is installed in a Voice Messaging configuration.
- One Cisco Unity server is designated the primary server, and the other Cisco Unity server is designated the secondary (or standby) server.

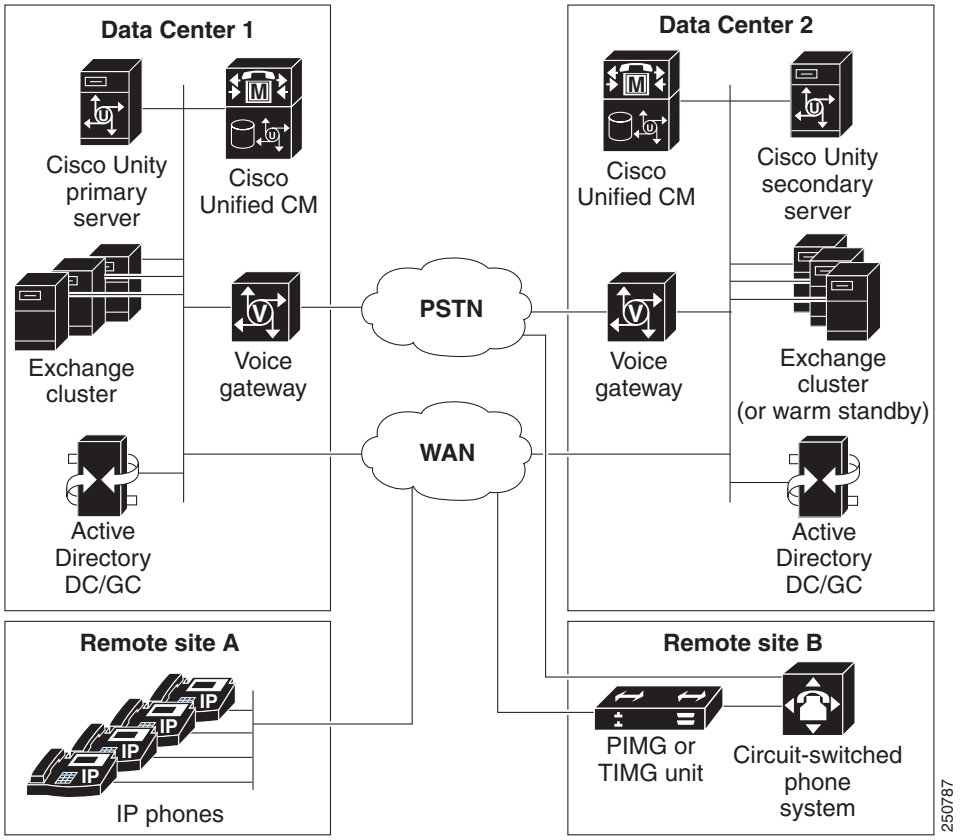
- Both Cisco Unity servers must appear on the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html and must belong to the same platform overlay.
- There must be a connection of 100 Mbps between the primary and secondary Cisco Unity servers.
- The network must meet the requirements listed in the "Network Requirements" section of *System Requirements for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/docs/voice_ip_comm/unity/5x/requirements/50cusysreq.html.
- If the Cisco Unity servers are being installed into an existing forest, both data centers must have one or more DC/GCs and one or more DNS servers.

  If the Cisco Unity servers are being installed into a new forest, both must be DC/GCs in the same Active Directory domain.
- The names of both Cisco Unity servers must be 14 characters or shorter.
- Exchange Server 2003 administration must be installed on the secondary server.
- Both Cisco Unity servers must have the same enabled features and configurations.
- SQL Server 2000 Standard Edition must be installed on both Cisco Unity servers. (MSDE 2000 is not supported on either server with Cisco Unity standby redundancy.)
- The SQL Server 2000 services MSSQLSERVER and SQLSERVERAGENT on both Cisco Unity servers must be configured to log on as the same domain account, and the account must belong to the Local Administrators group on each server. SQLSERVERAGENT on the primary server must be able to log on to SQL Server on the secondary server by using Windows NT authentication.
- All software must be installed on the same drive and directories for both primary and secondary servers.
- The Cisco Unity servers must have Cisco Unity 5.0(1) ES1 installed.

Diagram of a Standby Redundancy Configuration

Figure 7-1 shows one possible configuration for a Cisco Unity standby redundancy system.

Figure 7-1 Cisco Unity Standby Redundancy Example Diagram



CHAPTER 8

Voice-Recognition Access to Cisco Unity

The Cisco Unity voice-recognition feature lets users navigate the Cisco Unity conversation and manage voice messages by using spoken commands, either by saying the number associated with a menu option or by saying a word or phrase, for example, “play new messages” or “reply to all.”

For more information, see the following documentation:

- System requirements for voice recognition servers are listed in *System Requirements for Cisco Unity Release 5.0* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html.
- End-user documentation appears in:
  - The “Using the Press-or-Say Phone Input Style” chapter in the *User Guide for the Cisco Unity Phone Interface (Release 5.x with Microsoft Exchange)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_user_guide_list.html.
  - The *Release Notes for Spoken Commands in Cisco Unity 5.0(1)* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html.

Note the following about speech access to Cisco Unity:

- There must be a one-to-one correlation between voice-recognition servers and Cisco Unity servers that home subscribers with speech access to Cisco Unity. If Cisco Unity failover is configured, only one voice-recognition server is required for each pair of failover servers.
- A maximum of 24 voice-recognition ports are supported on Cisco Unity voice-recognition servers. For a list of servers supported as voice-recognition servers, see the *Cisco Unity Supported Platforms List* at http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html.
- The Cisco Unity server and the corresponding voice-recognition server must be connected across a high-speed IP network with minimal propagation delay and with proper Quality of Service guarantees for traffic between the components.
- The Cisco Unity server cannot be separated by a firewall from a Cisco Unity voice-recognition server. In a failover or standby-redundancy configuration, neither Cisco Unity server can be separated by a firewall from a Cisco Unity voice-recognition server.
- For voice recognition to be available on a Cisco Unity server, the license installed on the Cisco Unity server must include one of the following:
  - Unified Messaging subscriber licenses
  - Voice Messaging subscriber licenses with licenses for advanced features
- Voice recognition is currently available only in U.S. English.

CHAPTER 9

Migrating to Cisco Unity from Another Voice-Messaging System

When the customer is replacing another voice messaging system with Cisco Unity, consider the following:

- How do users interact with each system? For example, the options offered by the Cisco Unity standard conversation (the telephone user interface, or TUI), and the key presses used to accomplish tasks, may be different from what users are accustomed to using. As an alternative to the Cisco Unity standard conversation, some customers may want to activate Optional Conversation 1 (the ARIA-like conversation available in Cisco Unity) so that Cisco Unity subscribers hear message-retrieval menus that more closely resemble the choices they are familiar with. However, other menus—those that outside callers and Cisco Unity subscribers use to send and manage messages, as well as the menus that subscribers use to change their Cisco Unity settings—are the same as those in the Cisco Unity standard conversation.
- Ensure that the customer understands Cisco Unity behaviors that are different from those of the voice messaging system it is replacing. For example, if the customer does not currently use an automated attendant feature and wants Cisco Unity to be configured the same way, this should be noted so that the installer configures Cisco Unity correctly. If it is necessary to change any Cisco Unity behavior, such as the opening greeting, or zeroing out to an operator option during a personal greeting, these changes should be made and tested prior to the day of the cutover.
- Plan a method for creating Cisco Unity subscribers. Will they be imported from the message store (Domino or Exchange), imported from a text file (Exchange only), or added by using the Cisco Unity Administrator (Exchange only)? If they will be imported from a text file or added by using the Cisco Unity Administrator, where will the information come from? Creating subscriber accounts requires planning and testing prior to the cutover.
- The larger the installation or number of servers, the greater the need to perform subscriber enrollment tasks prior to the day of the cutover. If too many subscribers try to enroll simultaneously, some subscribers (up to the number of voice ports available) will succeed in accessing the Cisco Unity server and enrolling, but the rest will get a busy signal.

  To prevent this negative user experience, smaller groups of subscribers should be told, perhaps a few days in advance, how to call the pilot number and enroll in Cisco Unity before the system goes live.
- If the customer has special audio-text applications set up in the existing voice messaging system, Cisco Unity equivalents should be planned and set up before cutover. Cisco Unity supports audio-text applications and provides tools for designing and configuring them.
- Cisco Unity does not support group mailboxes, but the same functionality can be made available by setting up a call handler whose greeting prompts the caller to “press 1 for Pat, press 2 for Chris,” and so on.

- The supporting infrastructure (for example, message store servers), whether dedicated to Cisco Unity or being used by Cisco Unity, must be evaluated for availability and responsiveness. This can be accomplished by helping a customer understand the dependencies Cisco Unity has on the infrastructure, and how Cisco Unity performance or functionality can be affected by loss of connectivity to any of the external dependencies. Any problem areas should be addressed prior to installation of Cisco Unity. Cisco Unity will expose any deficiencies on the network, due to the way it uses the resources available on the network.

When the Cisco Unity design is finalized and verified through lab qualification, Cisco Unity functionality should also be tested before cutover by running a simulated load test and by running application test plans.

INDEX

A

alternate extensions 6-32
alternate MWIs 6-33
audio codecs
  affect on file size 3-5
  overview 3-5

C

centralized voice messaging 6-34
Cisco Unified Communications Manager
  authentication and encryption 6-12
  integrating Cisco Unity with multiple clusters 6-12
  integration with Cisco Unity 6-10
  packetization 6-17
Cisco Unified Communications Manager Express
  integrating with Cisco Unity 6-17
  multiple routers integrating with a single Cisco Unity server 6-19
Cisco Unity servers
  maximum number of users 3-4
  number of voice ports 3-4
  number required 2-4
  sizing and scaling 3-3
  storage capacity for voice messages 3-4

D

data storage
  configuration settings 2-10
  messages from outside callers 2-10
  subscriber information 2-7
  synchronization 2-9
  voice messages 2-6
domain controller, access and availability 3-2
Domino
  Active Directory accounts and permissions 5-6
  address book 5-8
  address book server 5-4
  address book terminology 5-2
  authentication 5-6
  changes that csAdmin makes to Domino Address Book 5-3
  changes that csClient makes to the Mail File 5-4
  client access licenses 5-8
  clusters 5-7
  criteria for supported configurations 5-10
  deployment
    administrative access and control 5-12
    establishing support policies 5-12
    network services 5-12
    operational tasks 5-13
    options 5-11
    Unified Messaging configuration tasks 5-12
  DUC for Cisco 5-2
  feature parity with Cisco Unity for Exchange 5-14
  mail drop server 5-4
  maximum number of subscribers allowed 5-2
  message routing 5-8
  message store server 5-4
  overview 5-1
  permissions 5-7
  server placement 5-5
  Unified Messaging configurations 5-9
  Voice Messaging configuration 5-10

E

Exchange
- Active Directory considerations 4-5
- considerations 4-7
- considerations with Exchange 2007 4-8
- deployment models 4-1
- mixed Unified Messaging and Voice Messaging 4-2
- Multi-site WAN with distributed messaging 4-3
- network infrastructure 4-4
- Unified Messaging with customer-provided infrastructure 4-2
- Voice Messaging with Cisco-provided infrastructure 4-2
- Voice Messaging with customer-provided infrastructure 4-3

F

failover
- compared to standby redundancy 7-1
- configuring when servers are separated by a firewall 7-2
- deploying between two data centers 7-2
- Voice Messaging configuration 7-2

firewalls 3-3

H

hardware components 2-3

I

interoperability 3-6

M

message store servers, availability 3-2

migrating to Cisco Unity, potential issues 9-1

multiple phone system integrations 6-30

N

name resolution 3-1

network connections 2-5

network resources, availability 3-1

P

phone integration
- alternate extensions 6-32
- alternate MWIs 6-33
- call control 6-8
- call information exchanged 6-7
- centralized voice messaging 6-34
- Cisco Survivable Remote Site Telephony (Cisco SRST) 6-19
- Cisco Unified Communications Manager (by using SCCP or SIP) 6-10
- Cisco Unified Communications Manager Express 6-17
- general issues 6-9
- integrating with multiple phone systems 6-30
- lines and cables required 6-3
- overview 6-1
- PIMG/TIMG 6-24
- sample path for a phone call 6-8
- settings in phone system and in Cisco Unity 6-7
- SIP 6-22

PIMG/TIMG
- failback procedure 6-29
- increasing port capacity 6-28
- integration description 6-24
- multiple integration support 6-29
- setup and configuration 6-27
- support for Cisco Unity failover 6-28

S

SIP integration 6-22

speech access to Cisco Unity 8-1
standby redundancy
compared to failover 7-1
diagram 7-5
requirements 7-2
with Exchange 2003 7-3

U

Unified Messaging description 2-2

V

Voice Messaging description 2-2
voice recognition 8-1